NKL®
CASH HANDLING

V1 & V2

NKL AUTOBANK SAFES
AUDITLOK XLV ELECTRONICS

Typical JCM Models

Typical CashCode Models

SERVICE MANUAL

NKL® is a member of FireKing Security Group
101 Security Parkway — New Albany IN 47150 USA
Ph. 800.528.9900 or 812-948-8400
www.fireking.com

© 2009 FireKing® Security Group.
NKL®, FireKing®, and AuditLok® are registered trademarks of FireKing® Security Group.

Doc 801810 • Rev 7/2009

1 INTRODUCTION

AUTHORIZED PERSONNEL

This service manual is intended to be used only by personnel authorized to service NKL Autobank safes. Unauthorized service will void the safe warranty and/or service agreement. Possession or use of this manual by unauthorized personnel does not constitute authorization. For information about service authorization contact NKL Technical Service.

SCOPE

This manual supports NKL Autobank V1 and V2 bill validating safes with AuditLok XLV electronics. This manual contains abbreviated operation and programming instructions. Complete safe operating instructions are found in documentation supplied with the safe.

This manual contains basic theory of operation, troubleshooting help, repair instructions, and electrical and mechanical parts information.

The original version of this service manual was written in 2001 and it covered all Autobank safes with AuditLok XLV electronics. This updated edition covers the V1C, V1R, V2C and V2R products only. Other models now have their own service manuals. When working with V1R and/or V2R products connected to D8C or Max Vend controller, refer to the applicable service manual for those products. Contemporary manufacturing is assumed unless specifically noted otherwise.

AUDITLOK XLV

AuditLok XLV is an electronic access control and accounting package. This electronics is used on several safe models in various configurations. Users log in with an electronic key and PIN or User Number and PIN. Fingerprint access is also available with the optional biometric reader. Up to 99 users may be enrolled in any combination of six permission levels. All lock and vend parameters are programmable.

C AND R CONCEPT

Every AuditLok XLV system must have one controller (C) unit. If the system consists of only one safe, that safe must be a C-unit. If the system includes any additional safes, those safes must be remote (R) units. R-units cannot function without a C-unit. Up to 15 R-units may be controlled by one C-unit. R-units are connected to the C-unit by a data bus using shielded cat-5 cable.

SAFE HARDWARE

The Autobank family of products includes a complete line of vending and validation safes. Although vending safes are beyond the scope of this manual, they can serve as controller units (C-units) for V1R or V2R safes.

Vending Safes with AuditLok XLV

NKL offer D8C and Max Vend products in the Autobank product family. D8C or Max Vend can serve as controller for one or more V1R or V2R safes.

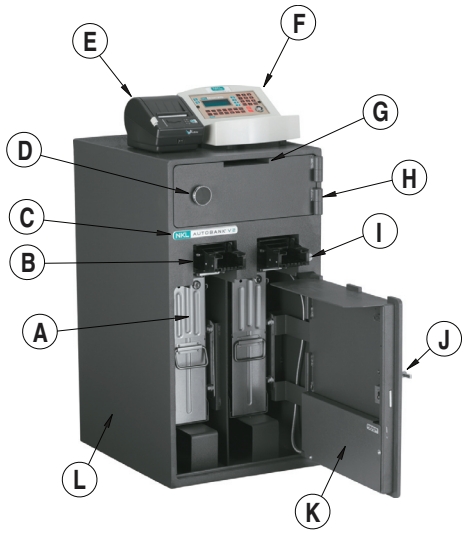
Validating Safes with AuditLok XLV

V1 safes have one bill validator. V2 safes have two bill validators. Various hardware configurations are available depending on the specific bill validator used. Units with CashCode (or older units with Mars) validators are 24 inches high, have one compartment, and are normally mounted on an 8 inch base to make the total height 32 inches. Units with JCM validators are a full 32 inches high and include a manual drop compartment with a slot (BNF style) or drawer (WBA style) in addition to the validator compartment.

V1 and V2 safes are available in C-unit and R-unit configurations. A V1C or V2C can serve as controller for one or more V1R or V2R safes. Communication between the C-unit and R-units is a critical function in multi-safe installations. Rules governing communication and communication settings in general apply equally to any C-unit.

NKL TECHNICAL SERVICE
PHONE 800-452-4655
WWW.FIREKING.COM

2 CHASSIS



A—VALIDATOR CASSETTE

Notes accepted by the validator are fed into a cassette where they are stored (JCM cassettes shown here). Style and capacity depends on validator.

B—BILL VALIDATOR

V1 and V2 safes may be equipped with Mars, CashCode, or either of two styles of JCM validator. A safe equipped with one type of validator cannot be converted to another type due to variations in hardware design.

Mars: NKL discontinued using Mars 3900 Series validators in 2003. Mars 3900 is a single-note feed with back-load 1200 cassette (lockable or high-security).

CashCode: Single-note feed with back-load 1500 note cassette (lock optional). CashCode validators are ideal for applications requiring high reliability and durability at a low cost.

JCM "BNF" (JBS Chassis): Bulk-note feed with reject tray and front load 2000 note cassette. For maximum security and serviceability the validator head is replaceable without opening the validator door. BNF style JCM is ideal for applications handling high cash volume where drop speed and serviceability are premium requirements.

JCM "WBA" (JSD Chassis): Single-note feed with front load 2000 note cassette. WBA offers the high capacity cassette similar to the BNF, but without the added expense of the bulk-note feeder assembly.

C—LABEL

Safe logo.

D—MANUAL DROP DOOR

JCM models feature a manual drop compartment with a simple knob-operated slam-bolt lock.

E—THERMAL PRINTER

C-units include a thermal printer.

F—EPR KEYPAD/DISPLAY

The keypad/display module is mounted in an attractive counter-top housing called an EPR. The keypad itself features an e-key reader, a touch-membrane surface for protection from spills and a 20x4 fluorescent display.

G—MANUAL DROP

JBS models (JCM, Bulk-feed, slot) have a manual drop slot. JSD models (JCM, Single-feed, drawer) have a manual drop drawer. Other models do not offer a manual drop.

H—HINGE

Safes have welded hinges on which the door swings open, up to 180°. Do not attempt to clean hinges. Commercial cleaning chemicals will cause the hinge lubricant to break down, making it difficult to open or close the door.

I—ARMORED CAR SWITCH

This Medeco® key switch is used by armored car to fire the lock.

J—HANDLE

The "T" style handle on this safe turns 90° left (counter-clockwise) to open. When the handle is turned, its bolts retract and lock open. When the door shuts, a spring loaded detent mechanism fires the bolts to lock the door.

K—VALIDATOR COMPARTMENT DOOR

The door is made of 3/8 inch A-36 steel. It is laser cut for a perfect fit. It is equipped with a high quality, low profile boltwork for the best security and most efficient operation. The safe serial number is printed on the interior and exterior of the validator door.

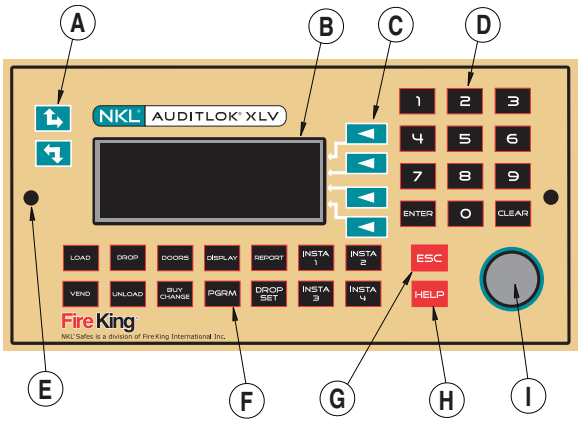
L—BODY

The body is 7 gage steel. All electrical connections via rear panel (not shown).

REAR PANEL

External power supply transformers, printer, and data cables connect to the rear panel of the safe.

3 AUDITLOK XLV KEYPAD/DISPLAY



A—SCROLL BUTTONS

Use on menu screens to scroll up or down or on certain screens to scroll left or right.

B—DISPLAY

This is an 80 character (4 rows, 20 columns) fluorescent display. It can easily be read at some distance in almost any lighting condition.

C—SELECT BUTTONS

Use to select menu items.

D—NUMERIC KEYPAD

This is a standard number pad. Use the **ENTER** button to accept an entered value. Use the **CLEAR** button to start over entering a number.

E—MOUNTING

For security the display module is mounted to the chassis or EPR using two Torx (T-25) security screws.

F—ACTION BUTTONS

Not all action buttons apply to every safe, but any given system could use almost any combination of action buttons depending on the application.

LOAD: Used only with vending safes.

VEND: Used only with vending safes.

DROP: Used when making manual or validated drops.

UNLOAD: Used only with vending safes.

DOORS: Used for door access.

BUY CHANGE: Used to vend change from a D8C or Max Vend in exchange for currency dropped into a validating safe.

DISPLAY: Check delays or error messages.

PGRM: Used to manage users or configure settings.

REPORT: Used to print any of several available reports.

DROP SET: Used to setup Insta-Drop and Extended Drop.

INSTA 1, 2, 3, 4: Used as a shortcut to initiate a validated drop.

G—ESC BUTTON

Used to cancel or end an action, back out of a menu, or from the idle screen use to access diagnostic and information menus.

H—HELP BUTTON

Not used.

I—KEY PORT

Present electronic keys to this reader port.

4 OPERATION

SERVICE OPERATION

Only those operations relevant to service are included here. Instructions are abbreviated for simplicity. It will be assumed during service that you have a User Number or key available with sufficient permission to perform the desired operation. If not, call NKL Technical Support to obtain log in instructions.

LOG IN

You must log in to perform most operations, including programming. Log in requires a User Number and a PIN, an electronic key and a PIN, or a fingerprint (if the system has a biometric reader). You may press the Action Button for the operation you are performing before or after these steps:

1. Present your electronic key or enter your User Number and press ENTER.
2. Enter your PIN.

VALIDATOR DROP

The main feature of a V1 or V2 safe is the ability to make validated drops. This is the standard validated drop procedure to be used for normal validator testing.

1. Log In.
2. Press DROP.
3. Select the name of the cash location where the drop is to be made.
4. Note the validator(s) switch on.
5. Insert notes. Currency should be accepted and stacked with the correct value displayed as it is accepted.
5. Press ESC to end the drop. The display may beep for a few seconds during the drop log-off process. A drop receipt should print automatically. Verify the receipt prints correctly and the correct drop amount is shown.

OPEN DOORS

In many cases it is necessary to open one or both doors for service purposes. Door delay and/or timelock may be set to zero for service purposes provided the settings are restored after service.

1. Log In.
2. Press DOORS.
3. When prompted to remove cash select NO.
4. Select the desired safe.
5. Select the desired door to open.

PRINT REPORTS

The Config Report and Cash Report are both very important for service. Various other receipts and reports, including the audit and other financial reports, are also useful for service under certain circumstances.

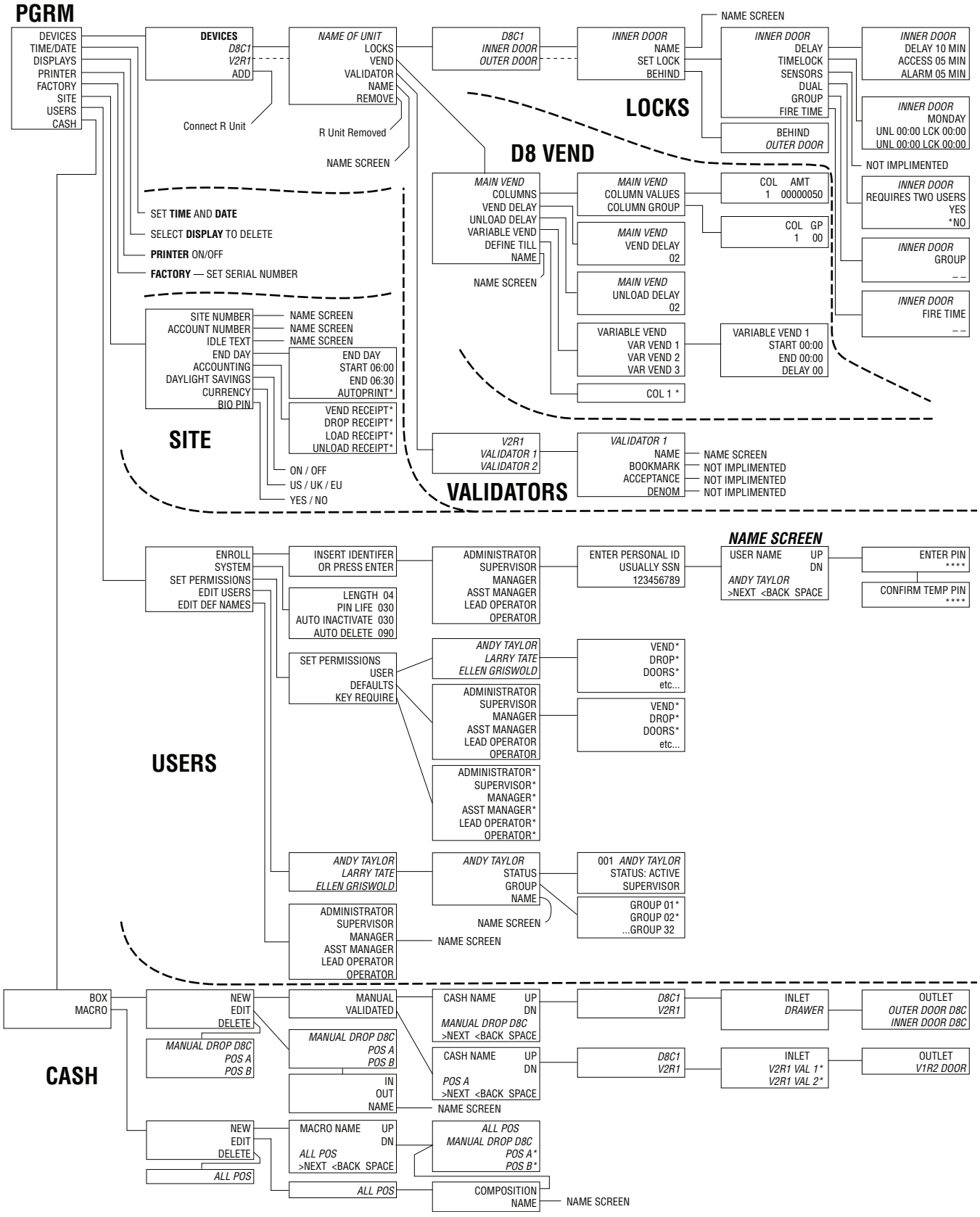
1. Log In.
2. Press REPORT.
3. Select the type of report to run.
4. Retrieve the report from the printer.

PROGRAMMING

Programming, particularly when replacing electronics, is critical to service and may include a wide range of settings.

1. Log In.
2. Press PGRM.
3. Choose the appropriate menu items to reach the desired parameters to set. Refer to the chart in Section 5 for guidance.

5 PROGRAMMING FLOW CHART



6 SETTINGS

PROGRAM – DEVICES

Name — A name is a 15 character text title stored in the CPU. Users, devices, locks, vend, validators, cashes and default permission levels have names.
Device — For practical purposes a device is a safe. A device is comprised of one or more locks and may have a hopper board, vend board, or one or two validators. Use the device menu to access lock, vend and validator settings.
Add Device — Add an R-unit to the system inventory.
Remove Device — Remove an R-unit from the system inventory (except EPR).

Lock Board Parameters

Lock — Each physical lock has its own lock board. All lock settings except the lock name and behind parameters are stored on the lock board.
Behind — When one door is physically behind another the Behind parameter lets the safe know this. This is how the safe knows to open the outer door before the inner door. Behind must be set to "none" unless the door is an inner door.
Door Delay — Requires user to log in and select the door to open or cash to remove, wait for the delay to complete, then repeat login and door/cash selection. The primary purpose is to serve as a robbery deterrent. Only one log in is required if Door Delay is set to zero.
Access Time — The period following a door delay during which the second login can be accomplished. Default value is 5 minutes.
Alarm Time — Maximum time a door may remain open after which an audible alarm sounds and a violation is logged in the audit. Default time is 5 minutes.
Fire Time — Safe doors with an ACO switch: This is how long you've got to activate the ACO switch; the value must be 1 minute or higher. Safe doors without an ACO switch: The lock remains energized for the designated time; set to zero to limit lock energized time to 7 seconds.
Timelock — The door may be accessed only during the period between UNL and LCK time. Set UNL and LCK to 00:00 to never enter timelock. Set UNL and LCK to 01:00 to put the door in permanent timelock. Only one timelock needs to be set per day to be active.
Dual — Enable dual to require two users with door permission to log in to open the door.
Group (Door) — Only users with door permission and who are assigned to the door's group may open that door.

Vend Parameters (D8C or Max Vend)

V1R/V2R safes may be controlled by a D8C or Max Vend as well as V1C or V2C. Specific vend parameters will be different when a Max Vend unit is in the system. Refer to the D8C or Max Vend service manuals for additional details regarding vending parameters.

Universal Interface Board (UIB) Parameters

Validator — Each validator has an associated UIB. Validator names are stored in the CPU. Acceptance and denomination restrictions are set on validator hardware.

PROGRAM – CLOCK

Time — System time is set in military format.
Date — System date is set in MM/DD/YY format.

PROGRAM – PRINTER

Printer ON/OFF — Printer must be set to ON to enable all vend, validator and other financial features.

PROGRAM – FACTORY

Serial Number — This is a five digit number assigned by NKL to the organization who owns the safe. The Serial Number must be correctly set in order to allow remote Edge software users to access the safe.

PROGRAM – SITE

Site Number — This appears on all reports and receipts. It should be set to the store number.
Account Number — This appears on Deposit Reports. The bank account number is necessary in order to produce a fully bank-ready deposit slip.
Idle Text — Set to the business name; appears at the top of the screen at idle.
End Day — If AUTOPRINT is ON: Sets the End Day Report to run automatically at the START END DAY time. If AUTOPRINT is OFF: Sets the message "RUN END DAY NOW" to appear on the screen from the START END DAY time until the End Day report is ran (or until the END END DAY time is reached) and allows any enrolled user to run the End Day Report regardless of their permission level. If the END END DAY time is reached, it switches off the RUN END DAY NOW screen message and cancels universal permission to run the End Day report.
Accounting (Receipt Print) — By default all receipts print automatically, however to conserve paper you may disable automatic printing of specific types of receipts.
Daylight Savings — If enabled, the system clock will automatically move forward or backward one hour on the proper date. Version 3.411 and higher CPU software supports the USA 2007 daylight savings time schedule. Older software versions support the pre-2007 USA daylight saving schedule.

6 SETTINGS

Currency — Sets the printed symbol for financial value to US ($), UK (£) or EURO (€).
Bio PIN — If a biometric reader is present, set to Yes to require users to enter their PIN after their fingerprint is read. This feature is only necessary for Duress alarm.

PROGRAM – CASH

Box Cash — Box Cash is defined as the financial value associated with a specific physical compartment. May be manual or validated. Defined by inlet (manual drop or one or two validators) and the outlet (lock) for the compartment. When opening doors the user is asked whether they are removing cash. If they answer yes, they select the name of the cash rather than the name of the door. Value is added to the cash when a user makes a drop (manual or validated). Value is reset to zero when the door physically opens and the user has chosen to remove cash. Configuring box cash requires creating a box cash name, assigning type (validated or manual), assign a safe, if validated assign validators, assign the safe door. No validated or manual drops can be calculated and validators will not function until box cash is fully and properly configured.
Macro Cash — Used by armored car to allow access to multiple validated box cashes with only one keypad operation. Macro Cash should only be setup if more than one validated box cash exists in the system. After configuring box cashes, create a macro, name the macro, then assign validated box cashes to the macro.

PROGRAM – USERS

User — Up to 99 users may be enrolled. Any user may be enrolled with any six available permission levels. The #8 ACO electronic key is hard-coded with its own unique permission. User 0 is the "Factory" user number. User 0 is automatically deleted once the first user is enrolled.
Identifier — User Number, electronic key, or fingerprint.
User Number — Number assigned sequentially as new users are enrolled. Keyless users must enter their User Number each time they log in to uniquely identify themselves.
Personal ID — This is a number up to 9-digits long assigned at the time a user is enrolled. It must be a different number for every user.
Permission Levels — The system has six progressive permission levels. A user may only enroll another user of equal or lower permission level. Each permission level has a default name which is editable.

Permissions — An exhaustive list of permissions is available for each permission level. Default permissions are established for each permission level including groups. Changing a permission for a level will not affect users already enrolled. Permissions for individual users are editable separately. For a complete list of possible permissions refer to the Permission Chart.
Key Require — Set based on permission level; if enabled for a given level, all users enrolled at that level may only be enrolled with an electronic key (or fingerprint).
PIN Length — Factory default is 4-digits. The alternate setting (6-digits) should not be selected except where required for high security applications.
PIN Life — Frequency in days that users must change their PIN.
Auto-Inactive — Number of days after a user's last log-in until their status is changed to inactive.
Auto-Delete — Number of days after a user's last log-in until their status is changed to deleted.

PERMISSION	ADMINISTRATOR	SUPERVISOR	MANAGER	ASST. MANAGER	LEAD OPERATOR	OPERATOR
Groups	00-05	00-05	00-05	00-01	00	00
Drop	✔	✔	✔	✔	✔	✔
Vend	✻	✻	✻	✻	✻	✻
Vend Till	✻	✻	✻	✻	✻	✻
Door	✻	✻	✻	✻	✻	
Report, User	✔	✔	✔	✔	✔	
Report, Cash	✔	✔	✔	✔		
Report, View Audit	✔	✔	✔	✔		
Report, Print Audit	✔	✔	✔	✔		
Report, End Day	✔	✔	✔	✔		
Report, Config	✔	✔	✔	✔		
Drop Set Delete	✔	✔	✔	✔		
Load	✔	✔	✔	✔		
Unload	✔	✔	✔	✔		
Edit/Delete User	✔	✔	✔	✔		
Enroll User	✔	✔	✔			
Set Vend Delay	✔	✔				
Set Unload Delay	✔	✔				
Set Var Vend	✔	✔				
Set PIN Length	✔	✔				
Set Timelock	✔	✔				
Set Delay	✔	✔				
Set Access	✔	✔				
Set Alarm	✔	✔				
Set Dual key	✔	✔				
Setup Cash	✔	✔				
Set Col Values	✔	✔				
Set Receipt Print	✔	✔				
Set End of Day	✔	✔				
Set Time	✔	✔				
Set Date	✔	✔				
Set Key Require	✔	✔				
Edit Permissions	✔					
Edit Default Permissions	✔					
Edit Permission Names	✔					
Set PIN Auto-Delete	✔					
Set PIN Auto-Inactive	✔					
Set PIN Life	✔					
Device Add	✔					
Device Delete	✔					
Device Name	✔					
Set Door Behind	✔					
Set Door Fire Time	✔					
Set Idle Text	✔					

✻*Access to components in assigned GROUPs.*

7 SYSTEM COMMUNICATION

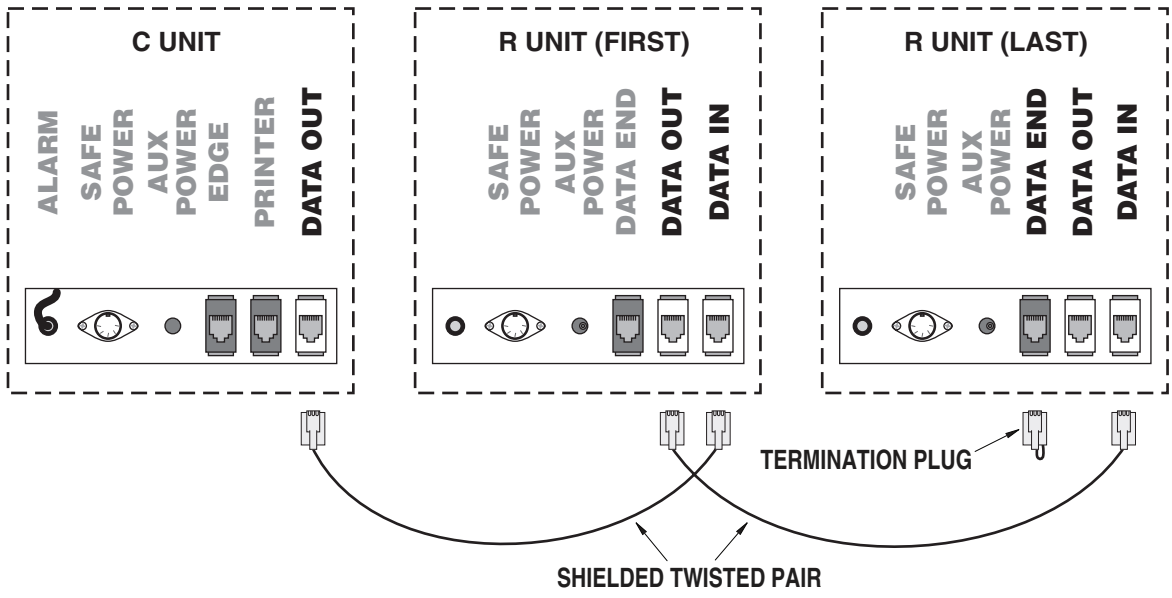
COMMUNICATION RULES

1. Up to 15 R-units (any combination of V1R and V2R), may be added to one C-unit.
2. Up to 4 displays (built in and EPR) may be connected to the system.
3. All R-units, including EPRs (after the first display), must be added using the Add Device procedure.
4. As soon as an R-unit is added, that R-unit is available on the Device Menu list to configure and use.
5. Once an R-unit is added, it will no longer respond to an Add Device request (until it receives a Remove Device command).
6. One display at Display Address 00 will communicate with the CPU. Only one display may be at Display 00. Any additional displays in the system are treated like R-units and must be added before they will communicate properly.
7. The rated maximum data bus length is 300 feet. Actual maximum length depends on wire quality, routing, and the presence of electronic noise in the environment.
8. S/N SP2008032034 and later (or upgraded older safes): Use shielded twisted pair for all data bus connections. The data bus must always be properly terminated to protect against electronic noise interference. A termination plug must be plugged into the DATA END port on the last R-unit on the data bus (V1R, V2R or EPR).

ADD DEVICE

When a system includes one or more R-units there are times during the course of service, such as after certain electronics are replaced, when it is necessary to add an R-unit (or EPR) to the C-unit. Establish communication with a V1R, V2R, or EPR as follows:

1. All components must be powered. The data bus is not connected to the R-unit(s) to be added until directed.
2. Log In.
3. Press PGRM.
4. Select DEVICES.
5. Select ADD.
6. While the screen indicates ADD DEVICE NOW connect the data bus from the C-unit (DATA OUT) to the first R-unit (DATA IN).
7. If the system has one or more R-units already connected and communicating, connect the data bus from the last R-unit already connected (DATA OUT) to the next R-unit (DATA IN).
8. Connect the Terminator Plug to the DATA END port on the last R-unit on the data bus (furthest from the C-unit on the data bus). ***Note:*** *The DATA END jack does not exist on R-units built prior to serial number SP2008032034. On older R-units the termination plug is not required unless R-unit electronics are replaced.*



Example system with one C-unit and two R-units.
Communication connections form a data chain. Shielded twisted pair RJ45 cables are used.
A termination plug is connected to the DATA END port on the last R-unit on the data bus.

7 SYSTEM COMMUNICATION

REMOVE DEVICE

Before taking any action that involves or requires removing a V1R or V2R, run all necessary financial reports and in particular a Cash Report if possible. When the CPU is to be replaced, all R-units must be removed first, if possible. If that is not possible the R-units must be removed by factory override after the CPU is replaced. When electronics are replaced in an R-unit, that R-unit must be removed (from C-unit inventory) before attempting to add the replacement electronics. R-units must have power when being removed regardless of the means.

Normal Remove Device (V1R/V2R) Procedure

The V1R and V2R-units being removed must be connected to the C-unit via data bus for it to receive the Remove Device command.

1. Log In.
2. Press PGRM.
3. Select DEVICES.
4. Select the V1R or V2R to be removed.
5. Select REMOVE.
6. The selected R-unit is no longer in the inventory of the C-unit. If it was properly connected and communicating at the time, it received the Remove Device command and is now available to be added to a C-unit. The data bus should be disconnected after all devices are removed.

Remove Device (V1R/V2R/EPR) by Override

The V1R, V2R or EPR units being removed must be connected to the C-unit via data bus for it to receive the Remove Device command. For additional information about overrides refer to Section 10.

1. Contact NKL Technical Service (1.800.452.4655) when you are physically in front of the safe.
2. The NKL technician will guide you through performance of the “50” override.
3. After the override is complete, disconnect the data bus to all R-units (do not disconnect Display 00 if it is mounted in an EPR case).

Normal Remove Display (EPR) Procedure

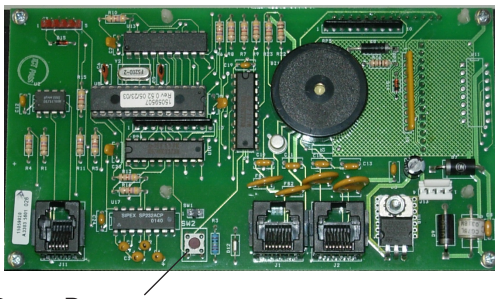
Since EPRs have no configurable settings they do not appear on the DEVICE menu. Use this procedure to remove a display from the C-unit inventory and, if it is connected to the C-unit at the time, its Display Address is reset to 00.

1. Log In.
2. Press PGRM.
3. Select DISPLAYS.
4. Select the display to be removed (Display 00 cannot be removed).
5. The selected display is no longer in the inventory of the C-unit. If it was properly connected and communicating at the time, it received the Remove Device command and is now available to be added to a C-unit. The data bus must be disconnected immediately after removing the display to avoid serious communication problems (you may remove power from the display if the data bus cannot be broken at this time).

Manual Reset to Remove Display (EPR)

Reset the software address of a Display manually if it is the main or only display (Display 00) and it will not respond; reset an auxiliary display if you are attempting to add it and it will not respond to the Add Device procedure (it should be removed from Display inventory before attempting to add it back in).

1. Remove the security screws holding the display to the safe front panel or EPR box.
2. If the display is built into the header disconnect the RJ45 cable from the can or if the display is in an EPR remove power from the EPR.
3. Press and hold down the reset button on the display circuit board.
4. Reconnect the display (RJ45 if header mounted or power if EPR mounted).
5. After 30 seconds release the reset button.
6. Cycle power to the display and test operation. If it is an auxiliary display it may now be added.

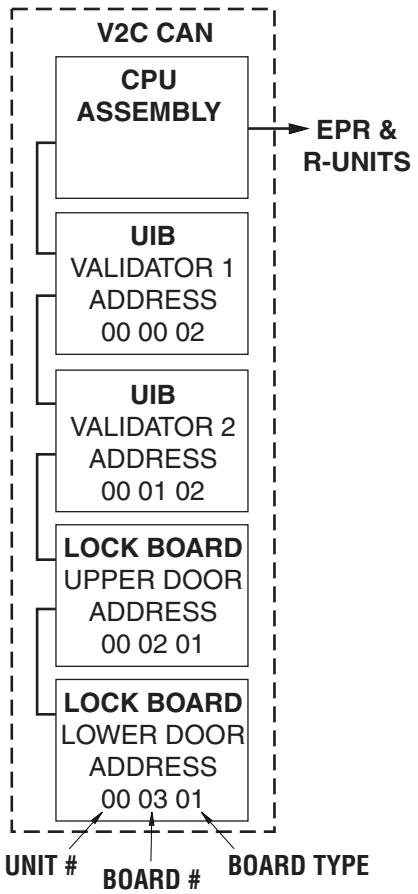


Display Board (Rear)

8 C-UNIT INTERNAL COMMUNICATION

COMMUNICATION RULES

1. Internal communication (CPU to UIB and Lock Boards) is established independently from any external (R-unit) communication using the Device Search procedure.
2. The primary display is at Display Address 00.
3. All R-units (except the primary display) must be disconnected when performing a Device Search.
4. The internal data bus consists of the connection from Daughter Board (CPU Assembly) J9 to the first UIB J1; from first UIB J2 to J1 on the next board on the bus and so on depending on the number of boards present. The last Lock Board on the bus will have J2 open.
5. The internal data bus must be terminated to protect against electrical noise interference. Terminate the data bus by setting SW1 Segment 8 to ON on the last Lock Board on the bus.
6. If the safe has any model of JCM validators (BNF, WBA, etc.): set SW2 Segment 1 to ON on each UIB. If the safe has any model of CashCode or Mars validator: set SW2 Segment 1 to OFF on each UIB.


V2C CAN
CPU ASSEMBLY
EPR & R-UNITS
UIB VALIDATOR 1 ADDRESS 00 00 02
UIB VALIDATOR 2 ADDRESS 00 01 02
LOCK BOARD UPPER DOOR ADDRESS 00 02 01
LOCK BOARD LOWER DOOR ADDRESS 00 03 01
UNIT #
BOARD #
BOARD TYPE

This example depicts a V2C with 2 Doors

DEVICE SEARCH

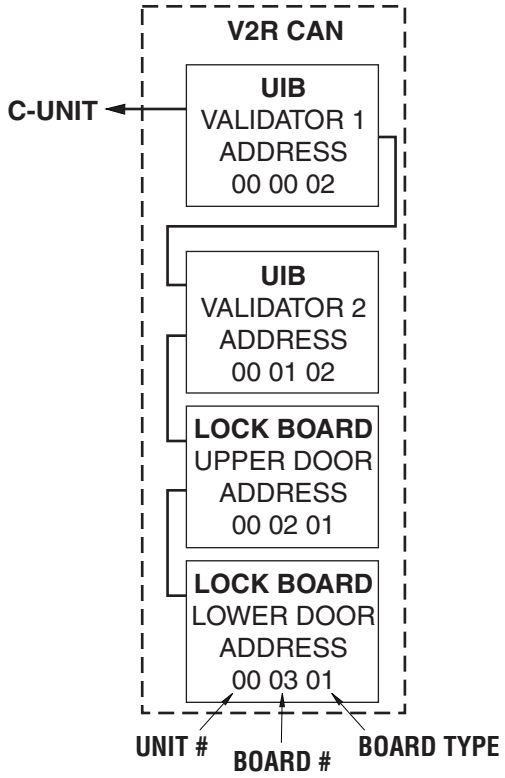
Perform a Device Search to establish C-unit internal soft addresses and internal device inventory (Section 10). A Device Search must be done after replacing the CPU, a UIB or a Lock Board (rather than replacing an entire can supplied by the factory) or if the CPU is not communicating with or otherwise not recognizing its internal device inventory (Section 10). The Device Search establishes communication between the CPU and all boards inside the C-unit.

1. Print End Day, Enrolled User, and Configuration reports if possible.
2. Disconnect all R-units from the data bus (primary display EPR must remain connected).
3. Remove power from the C-unit safe.
4. On the first Lock Board set SW1 Segment 1 to ON.
5. On the second Lock Board (if present) set SW1 Segments 1 and 6 to ON.
6. On the last lock board in the circuit (J1 or J2 will be open) set SW1 Segment 8 to ON.
7. On UIBs set SW2 Segment 8 to ON (Segment 1 must also be ON for JCM validators only).
8. Restore power.
9. Perform a “52” override (requires phone contact with NKL Technical Service: 1.800.452.4655).
10. Wait at least one full minute after the Device Search is complete.
11. Remove power.
12. Set Lock Board SW1 Segment 1 to OFF (all Lock Boards).
13. Set UIB SW2 Segment 8 to OFF (all UIBs).
14. Restore power. Wait at least one full minute (until the CPU full initializes) before continuing.
15. Check the inventory. Repeat this procedure if all boards in the C-unit are not found.
16. Reconnect R-units.

9 R-UNIT INTERNAL COMMUNICATION

COMMUNICATION RULES

1. Internal communication (UIB and Lock Boards) is established independently from any external (R-unit) communication using the Device Sync procedure.
2. R-unit electronics must be isolated from all external data bus connections while performing a Device Sync.
3. The internal data bus consists of the connection from the first UIB J2 to J1 on the next board on the bus; J2 on the second board to J1 on the third board (if present); then J2 on the third board to J1 on the fourth board (if present). J2 will be open on the last Lock Board on the bus.
4. The internal data bus must be terminated to protect against electrical noise interference. Terminate the data bus by setting SW1 Segment 8 to ON on the last Lock Board on the bus.
5. If the safe has any model of JCM validators (BNF, WBA, etc.) set SW2 Segment 1 to ON on each UIB. If the safe has any model of CashCode or Mars validator set SW2 Segment 1 to OFF on each UIB.



This example depicts a V2R with 2 Doors

UIB SYNC CHECK

Open the can (Section 14). Apply power to the can. Observe LEDs on the UIB(s) for proper sync indication:

1. V1R: Any two of the four LEDs will blink in a regular repeating pattern.
2. V2R: Any two of the four LEDs on one UIB will flash in a regular repeating pattern; the opposite two LEDs on the second UIB will also blink in a regular repeating pattern. The patterns do not have to match from one board to the other except that it must be opposite LED pairs blinking.
3. If the LEDs on a UIB blink randomly, are solid, or otherwise do not blink in a repeatable pattern as described above, replace the UIB. If both UIBs in a V2R are not indicating proper sync it may only be necessary to replace one, perform a Device Sync, and determine if the correct UIB was replaced by checking sync indicators again. In rare cases a Lock Board may be the cause of a sync check failure.

DEVICE SYNC

Perform a Device Sync to establish R-unit internal soft addresses and internal device inventory (Section 10). A Device Sync must be done after replacing a UIB or a Lock Board (rather than replacing an entire can supplied by the factory) or if a UIB Sync Check fails. Device Sync establishes communication between the UIB connected to the external data bus and all other boards inside the R-unit.

1. Print End Day, Enrolled User, and Configuration reports if possible.
2. Remove the R-unit (Section 7).
3. Disconnect the data bus from the R-unit.
4. Remove power from the R-unit.
5. Set Lock Board SW1 Segment 1 to ON (all lock boards).
6. On the second Lock Board (if present) set SW1 Segment 6 to ON.
7. On whichever is the last Lock Board (J2 or J1 open): set SW1 Segment 8 to ON.
8. Set UIB SW2 Segment 8 to ON (all UIBs)
9. Set UIB SW2 Segment 1 ON for JCM or OFF for CashCode or Mars validators.
9. Restore power.
10. Wait at least one full minute.
11. Perform the UIB Sync Check (above). If Sync Check fails, replace a different board and repeat Device Sync until the defective board is replaced.
12. Remove power.
13. Set Lock Board SW1 Segment 1 to OFF (all lock boards).
14. Set UIB SW2 Segment 8 to OFF (all UIBs).
15. Restore power to the safe. After one minute verify proper UIB Sync (above).

10 COMMUNICATION DIAGNOSTICS

SOFT ADDRESS

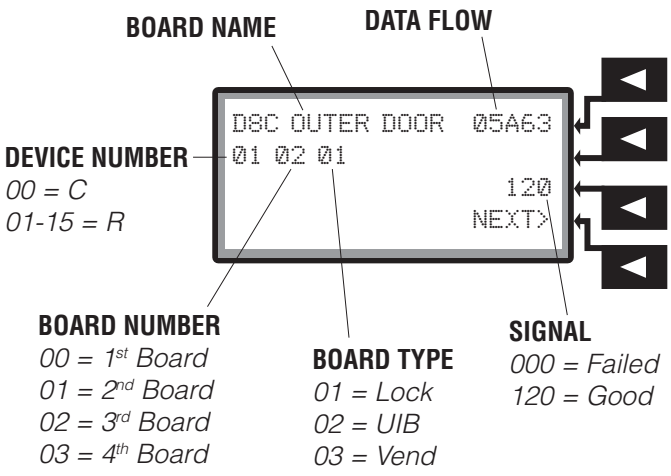
Lock boards, main vend boards and validator boards (UIBs) have a soft address made up of three parts. These parts include the unit number, board number, and board type.

Device Number — The C-unit is always Device 00. The first R-unit in inventory is Device 01, the second R-unit is Device 02, and so on.

Board Number (C-unit) — The first board found in a C-unit by the CPU during a Device Search is Board 00. The second board found is Board 01, the third is Board 02, and so on.

Board Number (R-unit) — The UIB connected to the external data bus is always Board 00. The next board is Board 01, the third is Board 02, and so on. Board 00 establishes its own inventory of boards inside the R-unit and reports this inventory to the CPU at the time the R-unit is added.

Board Type — A lock board is Type 01. A UIB (validator board) is Type 02. A main vend board is Type 03.



Device List / Diagnostic Screen

INVENTORY CHECK VIA DIAGNOSTIC

Check inventory and data bus communication using the Diagnostic screen:

1. At the idle screen press ESC.
2. Select DEVICES.
3. Interpret the information displayed as shown in the Device List /Diagnostic Screen example. *All other information beyond what is shown below may be ignored.* In the case of displays (shown at the end of the inventory cycle), only the Display Address is shown (Display Address is one two-digit number).
4. Select NEXT to cycle forward to the next board in the system.

INVENTORY CHECK VIA PRINT

One way to find the inventory of safes and circuit boards in a system is to run a Config Report (see Section 4). The Config Report will not list displays. A Config Report that is incomplete or prints with errors may indicate a communication problem.

Devices

Each time you find a line that includes the term "CONTROLLER" that line denotes the start of information about that unit. A V1 or V2 will appear as a VAL CONTROLLER (the first CONTROLLER listed is the C-unit). R-units are listed in Device Number order following the C-unit.

Boards

Each board is listed by name, type, and firmware version. The name is a 15-character user-defined text string. If a board has never been named it will have a 12-digit hexadecimal number as its name. The board type describes its function (LOCK, VEND, or UIB). After the CONTROLLER entry on the Config Report, each board is listed in order by Board Number.

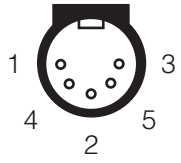
11 POWER

POWER SOURCES

One of the most common problems with electronic products is partial or complete loss of power. External power supplies are used with NKL safes so that a safe does not need to be drilled open to service the more common types of power supply failures.

Main Power Supply

The three-level main power supply transformer output (±12 V_{DC} and +5 V_{DC}) may easily be checked with a multimeter. The pin-out is shown below. To prevent power supply failure due to surges or spikes, always use an uninterruptible power supply (UPS) with your safe.



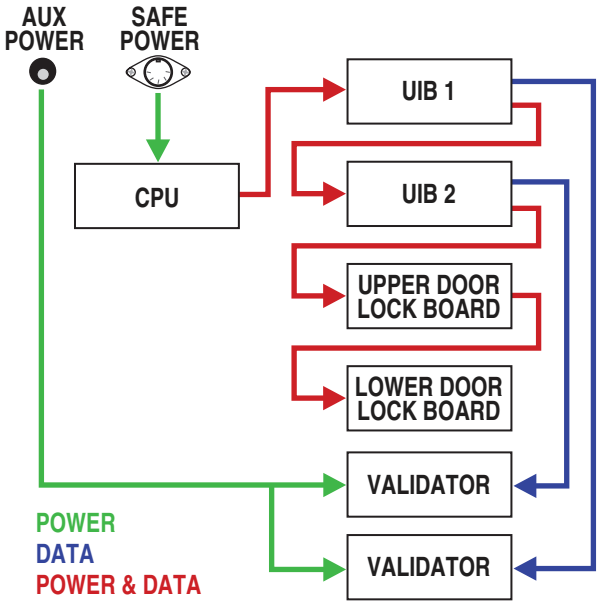
1 = COM
2 = COM
3 = +5 V_{DC}
4 = –12 V_{DC}
5 = +12 V_{DC}

Main Power Supply Connector Voltages

Validator "Aux Power" Supply

Safes with JCM or CashCode validators require a separate +12 V_{DC} (tip hot) external power supply. Older safes with Mars validators require a separate 24 V_{AC} external power supply. To prevent power supply failure due to surges or spikes, always use an uninterruptible power supply (UPS) with your safe.

JCM/CashCode Aux Power Connector Voltage



Internal Power Distribution (Before SP2009xxx)

POWER DISTRIBUTION

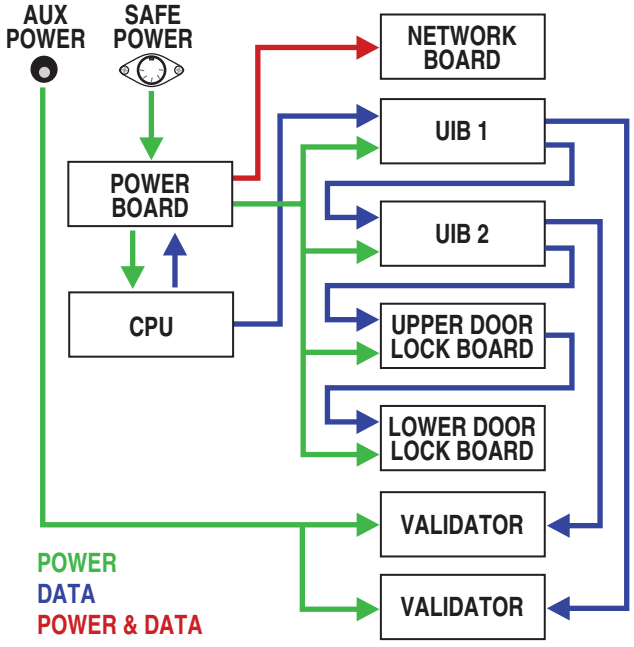
Safe Power is distributed to the electronics in the can to power each board. Prior to serial number SP2009xxx power and data were daisy-chained together. Units built after this serial number include a power distribution board so that power and data are routed separately. In either case, validators receive power separately from the Aux Power input.

Internal Power Distribution - Before SP2009xxx

The DC power input "Safe Power" from the rear panel feeds directly into the CPU assembly (C-unit) or the first UIB (R-unit). The first UIB on the internal data bus powers the remaining boards by passing power through each data cable on the circuit.

Internal Power Distribution - After SP2009xxx

The rear panel Safe Power input feeds into the Power Distribution Board inside the electronics can. This board distributes power to the CPU assembly (C-unit), Network Board (C-unit), and each UIB and Lock Board. In each case power is carried on a separate cable from the data. UIB and Lock Board data is connected in a daisy-chain. Each UIB and Lock Board receives power from its own power cable running back to the Power Board. In the case of the Network Board, RS232 data and power are carried on a common ribbon cable between the Power Board and Network Board.



Internal Power Distribution (After SP2009xxx)

12 ELECTRONICS CAN

CAN VS. BOARD REPLACEMENT

In most cases it is more cost/time effective to replace the electronics can regardless of which board inside the can is suspected of failure. Can replacement prevents having to perform the fairly tedious and time consuming task of performing a Device Search (Section 7) in a C-unit.

ELECTRONICS CAN

The electronics can contains the CPU assembly (C unit), the Lock Board(s), UIB(s), internal power harnesses, and other interconnecting cables. Cans produced since SP2009xxx also include a Power Distribution Board and a Network Board (C unit). When replacing an entire can, a new style can of the same configuration (C/R, number and type of validators, number of doors) can be used as a drop in replacement.

C-Unit Can Removal

Perform all of the following steps that are applicable and possible. The following procedure assumes the CPU is being replaced, whether individually or as part of a complete can replacement. If the CPU has failed steps 1 through 5 will not be possible.

1. Print a Config Report.
2. Print an Enrolled User Report.
3. Print an End Day Report.
4. If the system includes one or more R-units: Perform the Remove Device procedure (Section 7) to remove all V1R and V2R-units.
5. If the system has more than one EPR: Perform the Remove Display procedure (Section 7) to remove Display 01 and above.
6. Open the door(s).
7. Remove validator hardware as needed to gain access to the electronics can.
8. Disconnect cables to the can at the rear panel of the safe.
9. Disconnect cables to the can inside the safe.
10. Remove the 11/32 hex nuts holding the can in place.
11. Carefully pull the can out of the safe.

R-Unit Can Removal

The following procedure assumes the entire can is being replaced. Even when only one board inside the can is to be replaced, perform all of the following steps to ensure the customer's financial information is protected.

1. Print a Config Report.
2. Print an End Day Report.
3. Open the door(s) to this safe.
4. Perform the Remove Device procedure (Section 7) to remove this R-unit.
5. Disconnect power and data cables to the can at the rear panel of the safe.
6. Remove validator hardware as needed to gain access to the electronics can.
7. Disconnect cables to the can inside the safe.
8. Remove the 11/32 hex nuts holding the can in place.
9. Carefully pull the can out of the safe.

C-Unit Can Installation/Replacement

Perform the following steps when replacing the electronics can in a C-unit. If the CPU assembly or an individual board was replaced, follow the applicable procedure before performing this procedure.

1. Place the can in position over the mounting studs inside safe.
2. Reinstall the mounting nuts.
3. Reconnect internal lock and validator cables to the can.
4. Reinstall validator hardware as needed.
5. Reconnect the printer to the rear of the safe.
6. If applicable: Reconnect the Lantronix or external modem to the rear of the safe. Reconnect the alarm cable.
7. Reconnect the data bus to the EPR only. **DO NOT RECONNECT THE DATA BUS TO ANY V1R, V2R OR EPR DISPLAYS AT THIS TIME.**
8. Reconnect the main and aux power supplies. An audible door alarm may sound when the safe powers up. If so, ignore it. **DO NOT CLOSE ANY SAFE DOOR UNTIL DOOR OPERATION IS VERIFIED.**
9. Verify door operation before closing doors.
10. If the system includes R-units and/or additional displays: Perform the Add Device procedure (Section 7) to add the R-units (including extra displays) back to the system.
11. Print a Config Report.
12. Mark the Config Report with all of the differences from the pre-repair Config Report. This will allow you to see what settings must be reprogrammed.
13. Reprogram device settings as required. *In particular all board names will need to be entered. If the safe has two doors it may be necessary to try opening each door listed to verify which door is which.*
14. Create box cash for each manual and validated drop compartment.
15. Create macro cash made up of all validated drop box cashes if and only if the system includes more than one validating safe.
16. Print another Config Report and a Cash Report. Verify them against the originals and make any additional changes required.

12 ELECTRONICS CAN

R-Unit Can Installation/Replacement

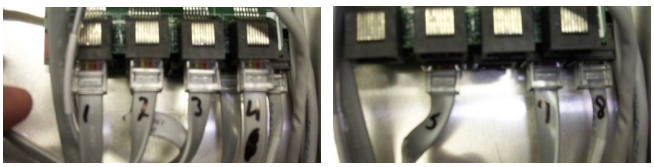
Perform the following steps when replacing the electronics can in an R-unit. If an individual lock board or UIB was replaced complete the Lock Board or UIB Replacement procedure before performing this procedure.

1. Place the can in position over the mounting studs inside safe.
2. Reinstall the mounting nuts.
3. Reconnect internal cables to the can.
4. Reinstall validator hardware as needed.
5. Reconnect the main and aux power supplies. An audible door alarm may sound when the safe powers up. If so, ignore it. **DO NOT CLOSE ANY SAFE DOOR UNTIL DOOR OPERATION IS VERIFIED.**
6. Verify door operation before closing doors.
7. Perform the Add Device procedure (Section 7) to add the R-unit back to the system.
8. Print a Config Report.
9. Mark the Config Report with all of the differences from the pre-repair Config Report. This will allow you to see what settings must be reprogrammed.
10. Reprogram device settings as required. *In particular all board names will need to be entered. If the safe has two doors it may be necessary to try opening each door listed to verify which door is which.*
11. Create box cash for each manual and validated drop compartment.
12. Edit macro cash to include this V1R or V2R validated box cash if and only if the system includes more than one validating safe.
13. Print another Config Report and a Cash Report. Verify them against the originals and make any additional changes required.

CPU ASSEMBLY REPLACEMENT

The CPU is the brain of an AuditLok XLV system. In any Autobank system, one safe in the system must have a CPU. The CPU in a C-unit can manage up to 15 R-units. The CPU assembly is comprised of the CPU top and bottom boards. These two boards always come as an assembly. Do not attempt to separate them or swap individual parts. The assembly is always mounted inside the electronics can of the C-unit. **ALWAYS OBSERVE PROPER GROUNDING AND STATIC PRECAUTIONS WHILE WORKING WITH EXPOSED ELECTRONICS.**

1. Perform the C-Unit Can Removal procedure (see above).
2. Remove the four small Phillips head screws from the can cover plate.
3. Remove the cover plate and set aside.
4. The CPU is a two-board assembly mounted toward the top (closest to the back panel connector plate). UIB and Lock Boards are mounted below the CPU.
5. Use a permanent marker to mark each cable connected to the top row of ports on the CPU assembly, then disconnect each of these.
6. Use a permanent marker to mark each cable connected to the bottom row of ports on the CPU assembly, then disconnect each of these.
7. Disconnect the power harness from the other side of the CPU assembly.
8. Remove the mounting screws from the CPU assembly and Remove old CPU.
9. Install the new CPU assembly and replace the mounting screws.
10. Reconnect the power harness and all RJ45 connections to the CPU.
11. Connect the EPR to the can.
12. Connect safe power to the can.
13. Check device inventory and if necessary perform a Device Search (Section 8).
14. Disconnect the EPR and power supplies.
15. Reinstall the can cover plate.
16. Perform the Can Installation/Replacement procedure (below).
17. Perform System Restoration (see below).
18. **DEFAULT NEW CPU LOGIN IS USER 0 AND PIN 1536.**



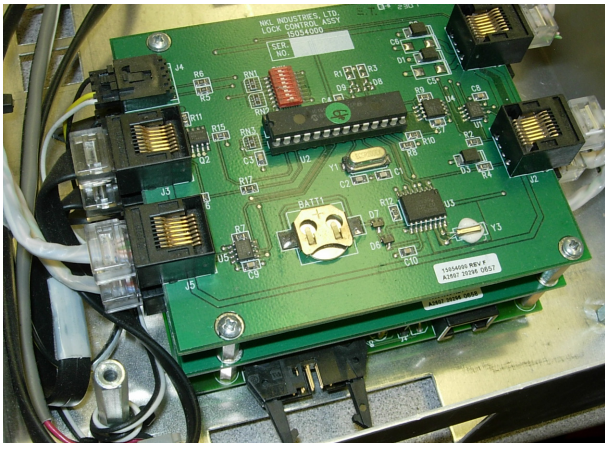
Top Row CPU Board Cables (shown left)
Bottom Row Daughter Board Cables (shown right)

12 ELECTRONICS CAN

LOCK BOARD OR UIB REPLACEMENT

Lock Boards and UIBs are mounted "sandwich style" in layers. UIBs are mounted to the bottom and Lock Boards are mounted to the top as you look into the open can. A safe with two doors will have two lock boards. A V1 will have one UIB and a V2 will have two UIBs. **ALWAYS OBSERVE PROPER GROUNDING AND STATIC PRECAUTIONS WHILE WORKING WITH EXPOSED ELECTRONICS.**

1. Perform the applicable Can Removal procedure (see above).
2. Remove the four small Phillips head screws from the can cover plate then set the cover plate aside.
3. Use a permanent marker to mark each cable as it is being removed in the steps to follow. Use these markings to ensure cables are reconnected properly later.
4. Disconnect all cables from the lock board(s) and UIB(s) to be removed (down to the affected board).
5. Remove the circuit board mounting screws.
6. Remove the top circuit board.
7. If necessary, continue removing standoffs and boards until the board to be replaced has been removed.
8. Replace the defective board and reinstall the standoffs, other boards, and mounting screws.
9. Reconnect all internal cables.
10. Terminate the data bus by setting SW1 Segment 8 to ON on the last Lock Board on the internal bus.
11. Set UIB SW2 Segment 1 to ON if using JCM validators or OFF if using CashCode or Mars validators.
12. C-Units Only: Connect the EPR to the can then perform a Device Search (Section 8).
12. R-Units Only: Perform Device Sync (Section 9).
13. Perform the applicable Can Installation/Replacement procedure (above).



Lock Boards and UIB's Mounted in Layers (One UIB and Two Lock Boards Shown Here)

POWER BOARD REPLACEMENT

This procedure is only applicable if the can has a Power Distribution Board (C-units SP2009xxx and above). This board is mounted to a special mounting plate designed to accommodate mounting above the CPU assembly.

1. Perform the Can Removal procedure (see above).
2. Remove the four small Phillips head screws from the can cover plate.
3. Remove the cover plate and set aside.
4. Mark each cable with a permanent marker to ensure cables are replaced in the correct position later.
5. Disconnect all cables from the Power Distribution Board.
6. Remove the mounting screws.
7. Replace the board.
8. Reverse this procedure to install the replacement Power Distribution Board.

NETWORK BOARD REPLACEMENT

This procedure is only applicable if a Network Board exists inside the can (C-units SP2009xxx and above).

1. Perform the Can Removal procedure (above).
2. Remove the four small Phillips head screws from the can cover plate.
3. Remove the cover plate and set aside.
4. Disconnect all cables from the Network board.
5. Remove the mounting screws.
6. Replace the Network board.
7. Reverse the above steps to reinstall the can and restore operation.
8. Refer to Section 13 to configure network settings.

CABLES

Cables seldom fail, however it is critical to connect cables properly. All RJ/RJ cables are "straight through" except for the lock cable(s) inside the can. Cable part numbers are clearly marked on most cables. Cables in new cans with a Power Distribution Board are color coded to help minimize confusion.

13 NETWORK INTERFACE

NETWORK INTERFACE

Many Autobank safe customers use NKL's Edge software to pull daily financial data from their safe. This requires proper configuration of the network interface.

Prior to serial number SP2009xxx

An external Lantronix network interface is used. It is connected via RS232 to the "EDGE" port (or "MODEM" port on older safes). The external Lantronix interface TCP/IP settings can be configured via RS232 or Ethernet.

Since serial number SP2009xxx

The network interface is installed inside the electronics can. The "EDGE" port is an Ethernet port. TCP/IP configuration requires an Ethernet connection to the safe.

Configuring the Network Interface via RS232

You must have a PC with the HyperTerminal application and an RS232 null modem cable (DB9-DB25) for an external Lantronix network interface or a special service use only cable (15050088) to configure an internal Network board.

1. Disconnect power from the Lantronix.
2. Connect the null modem cable from the RS232 port on the Lantronix to the RS232 port on your PC (internal board: connect special cable).
3. Start HyperTerminal. Set to serial port communication at 9600 baud, 8 data bits, no parity, 1 stop bit, flow control none.
4. Connect power to the Lantronix.
5. At the PC: Immediately press "x" (must be lower case) at least 3 times until Lantronix connection is indicated in HyperTerminal. If nothing appears in the HyperTerminal screen and the diagnostic light on the Lantronix goes off you missed the connection window. If this happens disconnect Lantronix power and start again from Step 4.
6. Immediately press ENTER.
7. At the menu type "0" then press ENTER.
8. Set the following (press ENTER to accept defaults if they are correct):
   - Enter the IP Address (assigned by the network administrator or obtained from NKL). The address is entered one segment at a time.
   - Set Subnet Mask to the number of host bits (normally 8).
   - If a Gateway is used set to Y, otherwise N.
   - Enter the Gateway IP Address (assigned by the network administrator or obtained from NKL). The address is entered one segment at a time.
10. At the menu type "1" and press ENTER.
11. Set the following (press ENTER to accept defaults if they are correct; order and list of variables may vary depending on specific Lantronix model, if any variables appear which are not listed here then simply accept the default value):
    - Baud rate = 9600.
    - I/F Mode = 4C.
    - Flow = 0.
    - Port = 3729.
    - Connect Mode = C0
    - Datagram Type = N/A
    - Remote IP = 0.0.0.0
    - Remote Port = 0
    - Pack Control = N/A
    - Disconnect Mode = 00
    - Flush Mode = 77
    - Disconnect Time = N/A
    - SendChar 1 = 0
    - SendChar 2 = 0
13. At the menu type "9" then press ENTER.
14. Disconnect the Lantronix from the PC. Connect it to the safe and the network.
15. Connect to the safe using the Edge software to verify operation.

Configuring the Network Interface via Ethernet

You must have the Lantronix device, a PC with Lantronix DeviceInstaller application (install from the CD provided with the Lantronix device), and both must be connected to the network.

1. Start the Lantronix DeviceInstaller application.
2. Click the Search icon to find the Lantronix device.
3. Select the Lantronix device from the appropriate folder.
4. Select the Web Configuration tab.
5. Click the Go button to start the Web Manager.
6. Select Network in the left navigation pane.
7. Configure Network settings as required: Select "Use the following IP configuration" and enter the IP Address, Subnet and Gateway (assigned by the network administrator or obtained from NKL); enable "Auto Negotiate".
8. Click OK.
9. Click Apply Settings in the left navigation pane.
10. Select Serial Settings in the left navigation pane.
11. Configure Serial Settings as required: Protocol RS232, Flow Control none, Baud 9600, Data bits 8, Parity none, Stop Bits 1, and set all Pack Control and Flush Mode options to No or disabled.
12. Click OK.
13. Click Apply Settings in the left navigation pane.
14. Select Connection in the left navigation pane.
15. Configure Connection settings as required: Protocol TCP, Accept Incoming yes with no password, Active Connect and Modem Mode none, Local Port 3729, Remote Port 0, Remote Host 0.0.0.0, TelnetMode disabled, Disconnect Mode default settings.
16. Click OK.
17. Click Apply Settings in the left navigation pane.
18. Close the DeviceInstaller application.
19. Connect via Edge software to verify operation.

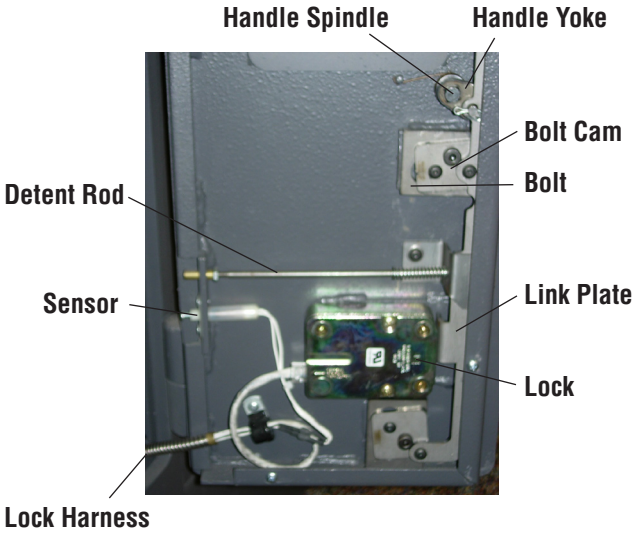
14 DOOR & LOCKING

COMPARTMENTS

All V1 and V2 safes have a validator compartment door. Certain chassis designs also have a manual drop compartment.

VALIDATOR DOOR

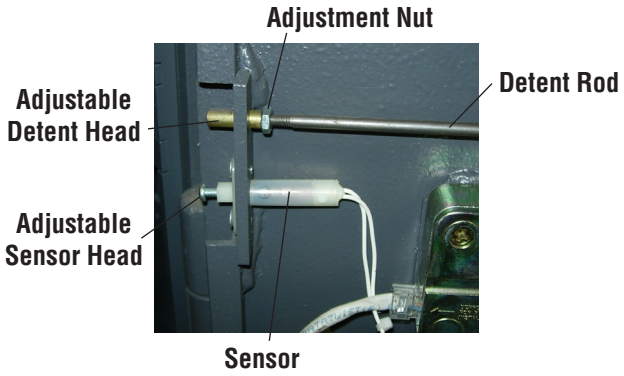
A slide-bolt lock is used on validator compartment doors today. Early safes used a LaGard swing-bolt lock. Either lock has an internal sensor to detect if the lock is in the locked position (bolts extended). An external plunger sensor detects door condition (open or shut). Lock and sensor cables are connected to the electronics can. The validator compartment door is equipped with a two-point or three-point "low profile" bolt work depending chassis design. The bolt work includes an automatic detent. Each bolt connects via cam to a link plate. The spring-loaded handle connects to the link plate via yoke. The detent consists of an adjustable spring-loaded rod activated from the hinge-side when the door closes.



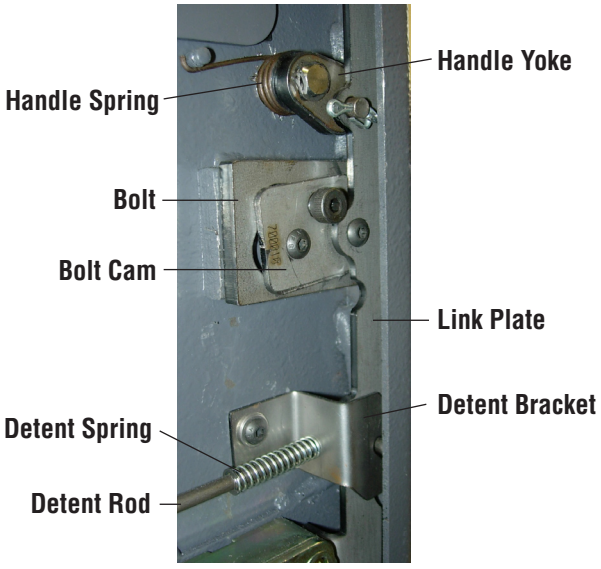
Typical Validator Compartment Door Hardware

DETENT ADJUSTMENT

To adjust the detent, loosen the hex nut behind the brass end piece, turn the end piece as needed, then tighten the hex nut in place. The detent should reliably catch and hold the bolts retracted when opening the door and should throw the bolts automatically when the exterior surface of the door is about flush with the chassis front surface.



Detent & Sensor Detail



Bolt Linkage Detail

MANUAL DROP DOOR

If present, this door will feature a simple knob operated spring-bolt lock. It will also have an adjustable magnetic plunger sensor similar to the one used on the validator compartment door.

HINGES

Doors are right-swing (hinges to the right as you look at the safe). Do not use chemical cleaners on hinges.

14 DOOR & LOCKING

CONTINUOUS DOOR ALARM

A continuous alarm tone sounds if a sensor indicates that a door is open more than five minutes (Alarm Time) or if a sensor detects a door come open or unlocked without a signal to energize the lock. For the validator compartment door this will happen if either the door plunger sensor or internal lock sensor activates. The manual drop compartment door is equipped with a plunger sensor only. Plunger sensors are adjustable.

Lock Sensor Test

Disconnect the lock cable at the lock. Measure continuity between pins 3 and 2 (normally open) at the RJ45 jack on the lock. When the lock is in the locked position the meter should indicate open. When the lock is in the unlocked position the meter should indicate closed. If the lock sensor fails replace the lock.

Door (Plunger) Sensor Test

A simple spring loaded plunger sensor is used to detect physical door status. The plunger switch is normally open. When the plunger switch is pressed (door shut), the plunger switch closes. Disconnect the sensor cable from the can or lock board before checking continuity.

DOOR NOT RESPONDING MESSAGE

The message “Door Not Responding” indicates an internal communication problem. If this occurs, first attempt power cycling the safe. If the problem continues, perform the inventory diagnostic and if necessary perform a Device Search (Section 8) or Device Sync (Section 9). If the problem persists, call NKL Technical Service to see if any other action can be taken before drilling the safe.

DOOR WILL NOT OPEN

Any of several things may be wrong: power, lock, cable, lock board, CPU, a configuration setting, or a mechanical problem.

Avoid the Drill When Possible

Drilling the door open is the last resort. If the door must be drilled, contact NKL Technical Service for drilling instructions. Drilling the door open will destroy the lock. After replacing the lock, test door operation with the door open (press and hold the door sensor to silence the alarm).

Internal Pressure

One possible problem is pressure against the inside of a door making it difficult to turn the handle. This problem can usually be overcome by pushing against the outside of the safe door while turning the handle.

Configuration Settings

Check and adjust lock settings:

1. Run a Config Report.
2. Verify that the all V1 or V2 safe doors are set Behind None.
3. Check the door delay and timelock settings. Check the safe clock. Correct any delay, timelock, or clock setting problems.
4. Set Fire Time to 01 (or higher if needed for the application).

LOCK BOARDS

Lock Boards are located inside the electronics can. A Lock Board may be replaced independently from other boards. If a Lock Board is replaced (as opposed to replacing the entire electronics can) it will usually be necessary to perform a Device Search (Section 8) or Device Sync (Section 9) to initialize internal communication.

Lock Board Output Test

This test checks the control voltage output from the lock board. The recommended measurement points are at the end of the lock cable (good cable continuity and internal crossover cable are assumed). Measure pins 6 and 8 at the end of the lock cable. The purpose of the test is to determine how much voltage is applied to energize the lock and for how long. With Fire Time set to 01 or higher the lock voltage (~ 12 V_{DC}) should only be applied to the validator compartment lock for a few seconds (approx. 7 seconds) after the Fire Switch (Armored Car Switch) is activated during Fire Time (Fire Time must be 01 or more). Voltage will remain applied to the manual drop compartment lock until Fire Time runs out or it senses the door open.

1. Check and if necessary set Fire Time to 01 (or higher for validator compartment).
2. Open the safe door.
3. Disconnect the lock cable at the lock.
4. Measure voltage at lock cable Pin 6 with reference to Pin 8. Normally the voltage should be zero. About 12 V_{DC} will appear when the lock is energized.

LOCK RE-TEST

Regardless of the part or parts replaced, verify proper lock and bolt work operation before closing the safe door.

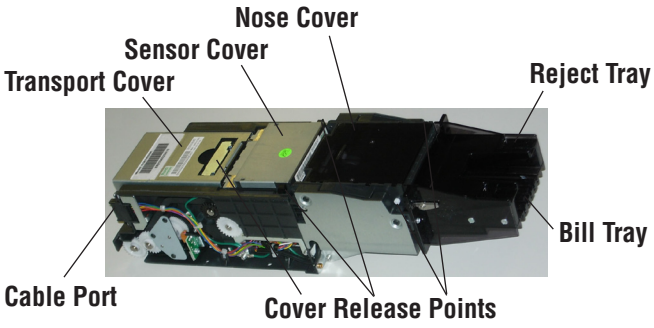
15 JCM VALIDATORS

GENERAL VALIDATOR OPERATION

Validators accept, count and store currency. Optic and magnetic sensors determine currency value and authenticity. Financial information (bill count, denomination, etc.) is transmitted from the validator to the UIB which in turn transmits it to the system CPU. Validating safes require an "Aux Power" supply to power the validator separately from "Safe Power."

JCM "BNF" VALIDATORS

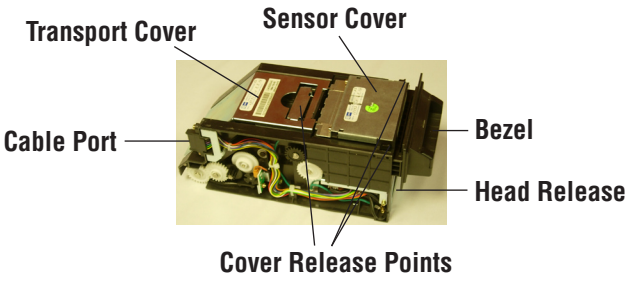
The BNF model validator features an extended head which can receive a small stack of bills and draw them in one at a time. The practical purpose is to save a cashier time by not requiring him or her feed in bills one at a time. Motors and sensors in the head pull bills through and validate them. If a bill fails validation it is rejected. Rejected bills go to a reject tray in the nose section to allow other bills in the feed tray to continue to be drawn in. The "front load" style cassette can be opened or removed from the front with the validator compartment door open.



"BNF" Validator Head

JCM "WBA" VALIDATORS

The WBA model validator is similar to the BNF model except it is single-note feed (accepts one note at a time). The WBA validator uses the same cassette hardware as the BNF although cassette bracket hardware is slightly different.



"WBA" Validator Head

CHASSIS DESIGNS

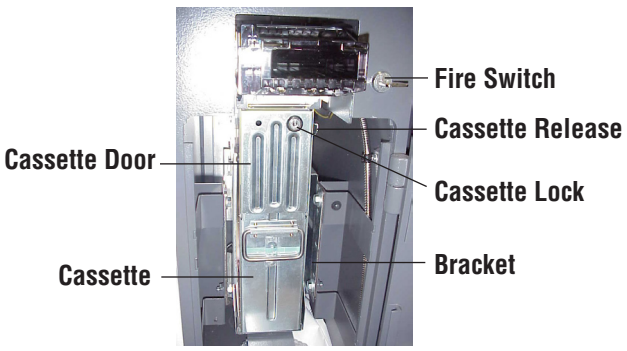
The chassis designs for WBA and BNF validators are slightly different, although technically you can insert either model validator head into either chassis. In both cases the chassis is designed to allow a JCM validator head to be removed for maintenance without exposing the cassette. Both designs feature a manual drop compartment. The JBS chassis has a drop slot whereas the JSD has a manual drop drawer. The cassette bracket assembly is shorter in the JSD in order to bring the WBA nose to the front of the safe. The cassette bracket for the JBS is set further back so that the BNF nose does not stick out as far.

V2C-JBS Chassis
"BNF" Validators

V2C-JSD Chassis
"WBA" Validators

CASSETTE ACCESS

With the validator compartment door open, unlock the validator cassette to open it and remove cash. The entire cassette may be removed by pressing down on the release lever located to the upper right as you look at the cassette. After pressing down on the release, pull out the cassette. Cassettes used in NKL safes are designed to hold a maximum of 2000 notes each.



Validator Compartment Interior

15 JCM VALIDATORS

ELECTRONICS CAN ACCESS

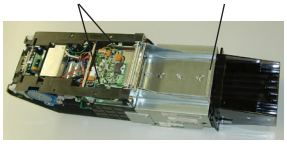
To reach the electronics can, the validator head, cassette, and bracket assembly must be removed. In a V2 you may only have to remove these parts from one side.

MAINTENANCE

Bill validators are wear items. Proper cleaning is a preventative measure that can substantially increase validator life. Insert a new cleaning card three times, then discard the cleaning card. Use a fresh cleaning card for each bill validator in the system. Use only NKL validator cleaning cards. Clear away light debris with dry compressed air and/or lint-free cloth. Never use alcohol.

BNF Head Removal/Replacement

The head may be pulled out of the safe without opening the safe door. The release is located under the nose section. Pull forward on the head release, then gently slide the entire head out of the safe. Use both hands for support because the validator head is heavy, particularly toward the back. When inserting, slide the head in slowly until it seats. When it seats properly the head release will catch. The validator will stack and nose lights will cycle three times then switch off (if Aux Power is connected and the cassette is installed).



Bottom of BNF Validator Head

Head Removal/Replacement

WBA Head Removal/Replacement

The head may be pulled out of the safe without opening the safe door. The release is located under the nose section. Press down on the head release and pull the head out slowly. Use both hands for support because the validator head is heavy, particularly toward the back. When inserting, slide the head in slowly until it seats. When it seats properly the head release will catch. The validator will stack and the red bezel light will come on and remain lit (if Aux Power is connected and the cassette is installed).

Setup

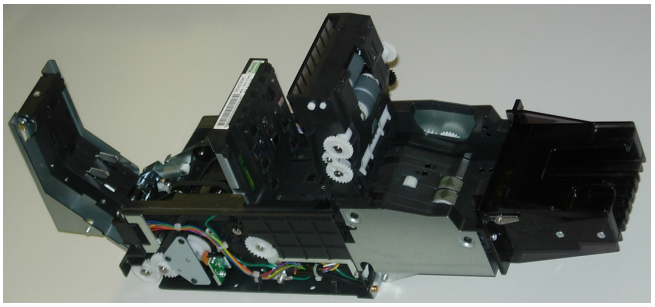
DIP switches on the validator head are used only for factory tests. For normal operation, all DIP switches must be in the OFF (up) position. Data and power from the electronics can are connected to the data port at the rear of the bracket assembly.

Stacker Test

The validator should automatically stack immediately when the cassette is seated if power is already applied or as soon as power is applied if the cassette is already seated. If it does not stack properly or makes unusual noises, check for a bill jam and if the problem persists, replace the validator.

Clearing a Bill Jam

1. Remove the validator head.
2. Open each section, examine the bill path, clear any debris, wipe as needed. and clean.
3. NEVER dig inside the bill path with tools. This will damage the validator. Never use alcohol as a cleaning agent - only use lint-free cloth (moist optional).
4. Reinstall the validator head.
5. Test operation.



Nose, Sensor, and Transport Sections Open

Bill Rejection

If bills are drawn in partially, then rejected, the bill is probably damaged (torn, stained, worn, etc.) or counterfeit. If the validator has problems accepting most or all bills, the optical reader is probably dirty or scratched (refer to cleaning instructions above). Inserting the same rejected bill repeatedly will eventually cause the validator to accept it. When this happens the bill will be recorded as an unknown denomination.

WBA Bezel Indicator Diagnostics

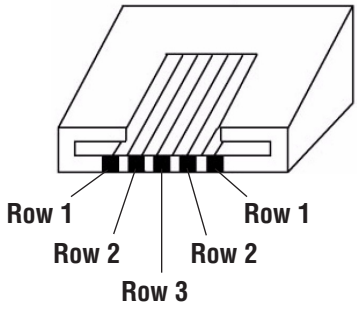
WBA lights come on only when ready to accept a bill. No flash codes exist for WBA.

15 JCM VALIDATORS

BNF Bezel Indicator Diagnostics

The BNF bezel has five lights. Row 1 is a set, Row 2 is a set, and Row 3 is an individual center light. If any of the flash codes cannot be corrected with the information below, replace the validator.

No lights: Idle (or no power).
All lights cycle in a constant repeating pattern: Ready to accept.
Cycle one time (Row 1, 2, 3, 1, 1): Normal power-up sequence.
2 Flashes on Rows 1 & 2: Bill jam (cassette stacker).
3 Flashes on Row 1: Bill jam (cassette stacker).
4 Flashes on Row 1: Bill jam (head or cassette).
4 Flashes on Rows 1 & 2: Bill jam (cassette stacker).
5 Flashes on Row 1 or Rows 1 & 2: Replace head.
6 Flashes on Row 1: Bill jam (head).
6 Flashes on Rows 1 & 2: Replace head.
7 Flashes on Row 1: Bill jam (head).
8 Flashes on Rows 1 & 2: Cassette full.
10 Flashes on Rows 1 & 2: Cassette not seated.
11 Flashes on Row 1: Replace head.
11 Flashes on Rows 1 & 2: Bill jam (cassette).
12 Flashes on Rows 1 & 2: Replace head.



BNF Bezel Indicators

Internal Electronics

There are no serviceable electronics in the validator head.

Currency Update

Replace the validator head.

Self-Test

There is no field “self-test” for JCM validators.

Unknown Denomination Error

The error message “UNKNOWN DENOM” may appear on the display or on a drop receipt. This message means the validator has accepted a bill but has not counted it. The only known cause is a power interruption during validation. This is most frequently due to intentionally cycling power as a corrective action for a jammed bill or similar maintenance.

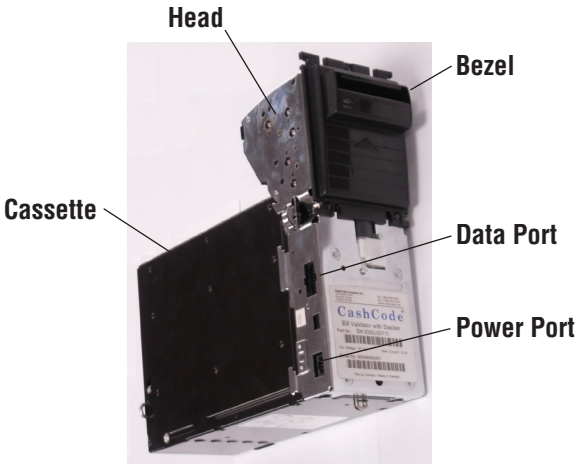
16 CASHCODE VALIDATORS

GENERAL VALIDATOR OPERATION

Validators accept, count and store currency. Optic and magnetic sensors determine currency value and authenticity. Financial information (bill count, denomination, etc.) is transmitted from the validator to the UIB which in turn transmits it to the system CPU. Validating safes require an "Aux Power" supply to power the validator separately from "Safe Power."

CashCode Validators

CashCode validators replaced the Mars 3900 Series as of late 2003. CashCode validators are single-note feed "back load" style. The validator is mounted to a bracket which is tilted down to allow access to the removable 1500 note cassette. Bills enter through the nose bezel then pass through the head assembly into the cassette. A motor on the validator drives the cassette's internal stacker to push notes from the bill path to the storage section.



CashCode Validator

CASSETTE ACCESS

Tilt the validator bracket assembly forward to allow access to the cassette. Squeeze the release actuators then lift the cassette off. The cassette will snap into place when reinstalling.

Cassette Release Tabs (Left)
Tilt and Lift Cassette to Remove (Right)

MAINTENANCE

Bill validators are wear items. Proper cleaning is a preventative measure that can substantially increase validator life. Insert a new cleaning card three times, then discard the cleaning card. Use a fresh cleaning card for each bill validator in the system. Use only NKL validator cleaning cards. Clear away light debris with dry compressed air and/or lint-free cloth. Never use alcohol.

Clearing a Bill Jam

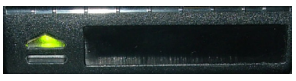
Bills may be rejected due to a torn bill or other object in the bill path, dirt, scratches or other damage to the sensor area, or worn belts or other moving parts.

1. Cycle Aux Power to force the stacking mechanism to cycle. This often forces a bill to pull through the stacker and elevator. Repeat once or twice, if needed.
2. Open the validator compartment.
3. Remove the validator cassette.
4. Press the head release button to expose the bill path. Examine the bill path, clear any debris, wipe as needed.
5. NEVER dig inside the bill path with tools. This will destroy the sensor heads. Never use alcohol as a cleaning agent - only use lint-free cloth (moist optional).
6. Put the cassette back on and verify it stacks. If not, there is a problem with the validator, cassette, or power supply.
7. Test operation by making a normal validated drop.

Head Open

Bezel Indicator Diagnostics

At rest the red bezel indicator is on and the green indicator is off. When enabled (ready to accept a note), the green bezel indicator is lit and the red indicator is off. If either bezel light blinks with a regular pattern there is a problem:



Green Light: Ready to Accept

Red Light: Idle

16 CASHCODE VALIDATORS

Flash Code:	Interpretation:
No Lights.....	No power.
Red On.....	Idle (not ready to accept bills).
Green On.....	Ready to accept bills.
Red Flashing.....	Cassette removed.
Red 3 Blinks.....	Cassette full.
Red 4-9 Blinks.....	Replace validator.
Red 11 Blinks.....	Bill Jam.
Red 12 Blinks.....	Bill stuck in cassette.
Green Flashing.....	Communication error.

Stacker Test

The validator should automatically stack immediately when the cassette is seated if power is already applied or as soon as power is applied if the cassette is already seated. If it does not stack properly or makes unusual noises, check for a bill jam and if the problem persists, replace the validator.

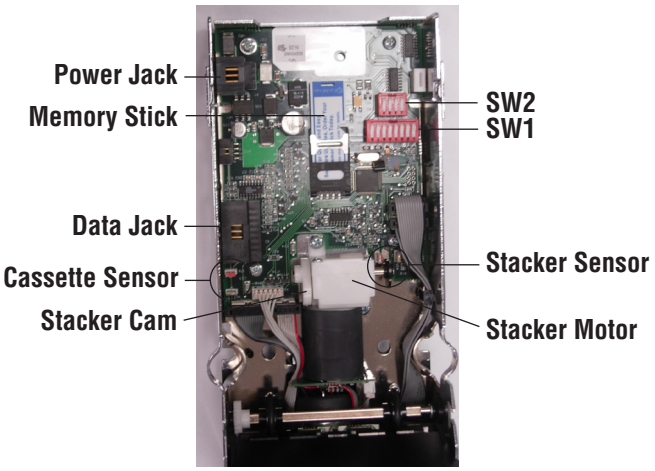
Internal Electronics

Remove the cover plate to access internal electronics. SW1 enables or disables currency denominations. Enable denominations as required. SW2 enables test mode, security level, and stacker direction. For normal operation set all SW2 switches to ON. Power must be cycled after making any changes to switch settings. A memory stick is used to load new software for updated currency support. Power must be removed when inserting or removing a memory stick. A “false” memory stick is normally installed to protect the electrical contacts.

Currency Update

From time to time the government issues new currency. In order to accept new currency, the validator must be updated (or replaced). To update a validator using a memory stick:

1. Open the validator compartment door.
2. Disconnect Aux Power.
3. Remove the cassette and electronics cover plate.
4. Insert the memory stick with the update in place of the protective “false” plastic strip.
5. Connect Aux Power.
6. Observe bezel lights flashing. After bezel lights stop flashing, the red light should be on solid.
7. Disconnect Aux Power.
8. Remove the memory and replace the protective plastic “false” stick.
9. Replace the electronics cover plate and cassette.
10. Connect Aux Power.
11. The validator should immediately stack.
12. Make a test drop using new currency to verify operation.



CashCode Validator Electronics Section

Self-Test

The self-test is a “go/no-go” test. If the validator will not accept a valid note in test mode (with the cassette on), the validator must be replaced.

1. Open the validator compartment door.
2. Disconnect Aux Power and Safe Power.
3. Disconnect the validator data cable at the can.
4. Remove the cassette and electronics cover plate.
5. Set Switch 4 on SW2 to OFF.
6. Replace the electronics cover plate and cassette.
7. Connect Aux Power.
8. The validator should immediately stack and the green bezel light should be lit. If not, replace the validator.
9. Insert a known good bill. If the validator still does not accept bills in test mode, replace the validator.
10. If a validator accepts bills in test mode, but not in normal operation, the problem is likely to be the data cable or the UIB.
11. Reverse the above to restore normal operation.

Replacement

Never connect or disconnect validator data cables unless power is removed to both the validator (12 V_{DC} Aux Power) and the main safe electronics (Safe Power).

1. Open the validator compartment door.
2. Disconnect Aux Power and Safe Power.
3. Disconnect data and power from the validator.
4. Remove the validator from its bracket assembly by removing the mounting nuts from behind the validator face.
5. Set all switches on the new validator to ON (disable currencies only if currencies were disabled on the validator being removed).
6. Reverse the above steps to install the replacement validator.
7. Verify the validator stacks properly. Make a test drop.

17 MARS VALIDATORS

GENERAL VALIDATOR OPERATION

Validators accept, count and store currency. Optic and magnetic sensors determine currency value and authenticity. Financial information (bill count, denomination, etc.) is transmitted from the validator to the UIB which in turn transmits it to the system CPU. Validating safes require an "Aux Power" supply to power the validator separately from "Safe Power."

Mars 3900 Series Validators

Mars 3900 Series validators (discontinued 2003) are "back load" style. The validator is mounted to a bracket which is tilted down to allow access to the removable (standard or high security) 1200 note cassette. Bills enter through the nose bezel, pass through the head assembly to the elevator section, then the stacker pushes the note into the cassette.

CASSETTE ACCESS

Tilt the validator bracket assembly forward to access the cassette. Rotate the knob to the "Remove" position. Tilt the cassette forward. Slide the cassette up then lift away. Reverse these steps to reinstall the cassette. The cassette knob must be fully in the "Engaged" position or the validator will not accept bills.

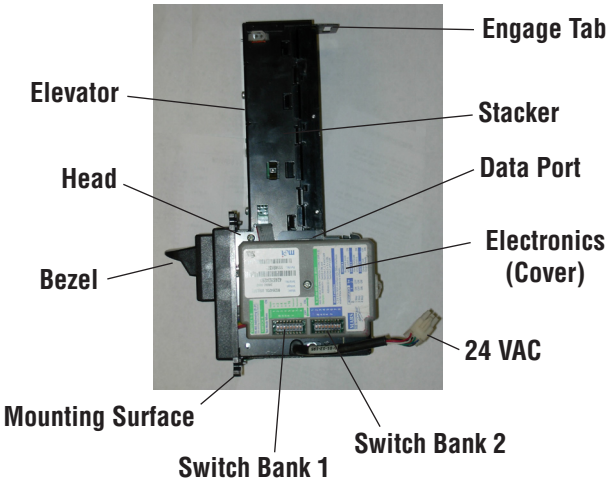
MAINTENANCE

Bill validators are wear items. Proper cleaning is a preventative measure that can substantially increase validator life. Insert a new cleaning card three times, then discard the cleaning card. Use a fresh cleaning card for each bill validator in the system. Use only NKL validator cleaning cards. To clear away light debris spray with dry compressed air only. Never use alcohol.

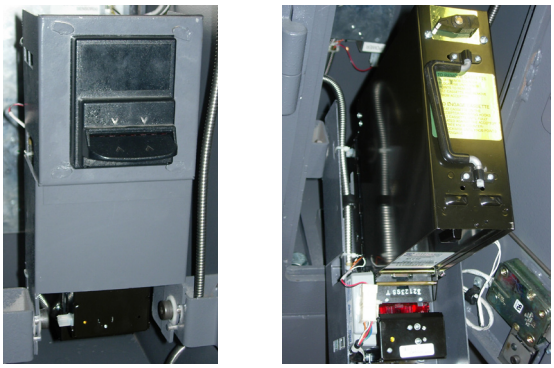
Clearing a Bill Jam

Bills may be rejected due to a torn bill or other object in the bill path, dirt, scratches or other damage to the sensor area, or worn belts or other moving parts.

1. Cycle validator power to force the stacking mechanism to cycle. This often forces a bill to pull through the stacker and elevator. Repeat once or twice, if needed.
2. If the bill (or foreign object such as tape or paper clip) remains stuck, it will be necessary to remove the validator cassette, dismount the validator, and remove the electronics case to access the bill path. If the obstruction cannot be found or cleared, replace the validator.
3. NEVER dig inside the bill path with tools. This will destroy the sensor heads.
4. Once the bill jam is cleared, cycle power to the safe to clear the error message if needed.



Mars Validator



Validator Bracket Assembly
Normal Operation Position (left)
Tilted Down for Cassette Access (right)

Tilt Cassette to Slide On or Off Validator

Switch Banks at Validator Electronics Cover

17 MARS VALIDATORS

Bezel Indicator Diagnostics

At rest the green bezel indicators are off and an internal red light (you must be eye level with the bill path) will flash two to three times each minute. When enabled (ready to accept a note), green bezel indicators will light solid (and the red internal light will also light solid) to indicate that the validator is ready to accept bills. If the bezel lights do not come on when making a drop, there is a problem with the validator, power, UIB, data bus, or system programming. To help determine the most likely cause of trouble, observe the validator bezel indicators for activity.

Flash Code:	Interpretation:
No Lights.....	Not ready or no power.
Steady On.....	Ready to accept bills.
Rapid Blinking.....	Cassette full.
3 Blinks.....	Coupon mode. Reset switches and power cycle.
4 Blinks.....	Bill jam.
5 Blinks.....	Cassette not engaged.
6 Blinks.....	Tamper detected. If the condition does not clear within 15 minutes, replace the validator.
7 Blinks.....	Stacker blockage. Remove the cassette and clear the stacker of debris. If the problem persists, replace the validator.
8 Blinks.....	Bill taken but no credit given. This may show up in a report as an unknown denomination. It is usually the result of a temporary power loss while making a drop.
9 or 10 Blinks.....	Dirty sensors. Use approved cleaning cards or dry compressed air.

Validator Bezel Lights

Stacker Test

When the cassette is properly engaged, the validator should automatically cycle its stacker a few seconds after it is powered up. If it does not stack properly or makes unusual noises, check for a bill jam and if the problem persists, replace the validator.

Self-Test

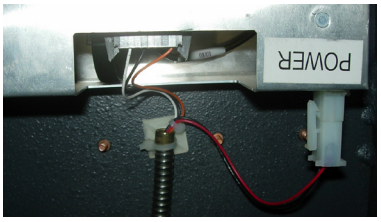
During normal operation all switches on both banks are in the OFF position. Set Switch 8 on Bank 1 to ON to put the validator in test mode. Changes to switch settings take effect only after the validator is power cycled. The self-test is a “go/no-go” test. If the validator will not accept a valid note in test mode with the cassette engaged, the validator must be replaced.

1. Remove power to the validator and safe.
2. Disconnect the data cable to the UIB.
3. The cassette must be installed (Engaged).
4. Set Switch 8 on Bank 1 to ON and all other switches OFF.
5. Apply power to the validator (it should immediately stack).
6. Insert a known good bill. If the validator still does not accept bills in test mode, replace the validator.
7. If a validator accepts bills in test mode, but not in normal operation, the problem is likely to be the data cable or the UIB.

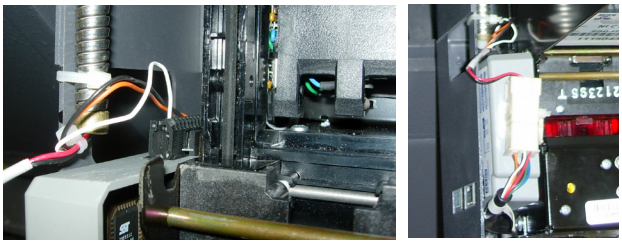
Replacement

Never connect or disconnect validator data cables unless power is removed to both the validator (24 V_{AC} Aux Power) and the main safe electronics (Safe Power).

1. After opening the validator compartment door remove Safe Power and Aux Power.
2. Disconnect data and power from the validator.
3. Remove the validator from its bracket assembly by removing the mounting nuts from behind the validator face.
4. Set all switches on the new validator to OFF.
5. Install the new validator onto the validator bracket.
6. Connect power and data cables.
7. Restore power to the safe and validator.
8. Check that the validator stacks. Make a test drop.



Power and Data Connections at Can



At Validator: Data Connection (Left)
Power Connection (Right)

18 HISTORY

PRODUCT HISTORY

The first V1 and V2 products were shipped from NKL late in the year 2000. As with any advanced technology product, these have seen numerous updates and changes over the years. The information in this manual has thus far been provided to assist with general service as if they were produced nearer the writing of this document. This section attempts to describe significant product updates over the life of the product.

UPDATES

For a complete list of updates and to download bulletins, including those written after the publication of this manual, refer to our web site:

http://www.fireking.com/techsup_safes_bulletins.html

Warranty Seal Sticker

Starting with SP2002019058 all V1/V2 safes had a "Warranty Void If Seal Broken" sticker on the dust cover.

XLV 2.0

Released Version 2.0 at SP2002020149.

Kaba Mas Lock

Started using the Kaba Mas outer door lock (15017000) in place of the LaGard lock (15016000) at SP2002023166.

XLV 2.0.4

Released Version 2.0.4 at SP2002026018.

New Display

Introduced new display board with a push-button reset switch instead of DIP switches at SP2002048148. This display (15059020) is interchangeable with its predecessor.

XLV 3.0.

Released Version 3.0. (June 2003, serial number not available). This is the first version of XLV software to support NKL Edge remote software.

Serial Number on Can

Began marking the can with the safe serial number at SP2003038151

Uninterruptable Power Supply

Added UPS with each "C" unit safe at SP2004006001. Stopped including UPS as a standard item at SP2004022003 (UPS is available as an option today).

Lock Board Firmware

Lock board firmware update (version 0.49) to correct a minor issue with timelock settings (August 2004).

XLV 3.37

Released XLV software 3.37 with minor code corrections at SP2004037064.

XLV 3.411

Released XLV version 3.411 at SP2007009051 to support 2007 USA Daylight Saving Time schedule change.

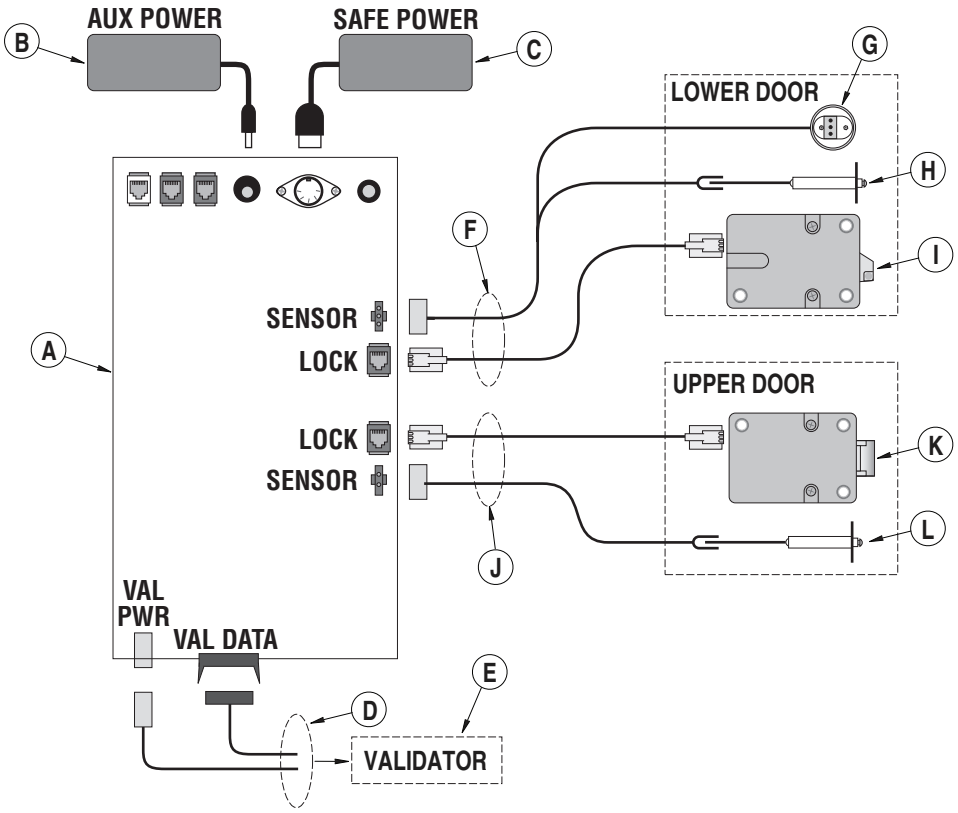
XLV 3.53

Released XLV version 3.53 at SP2008028180 (most updates are related to bill validation).

Data Bus

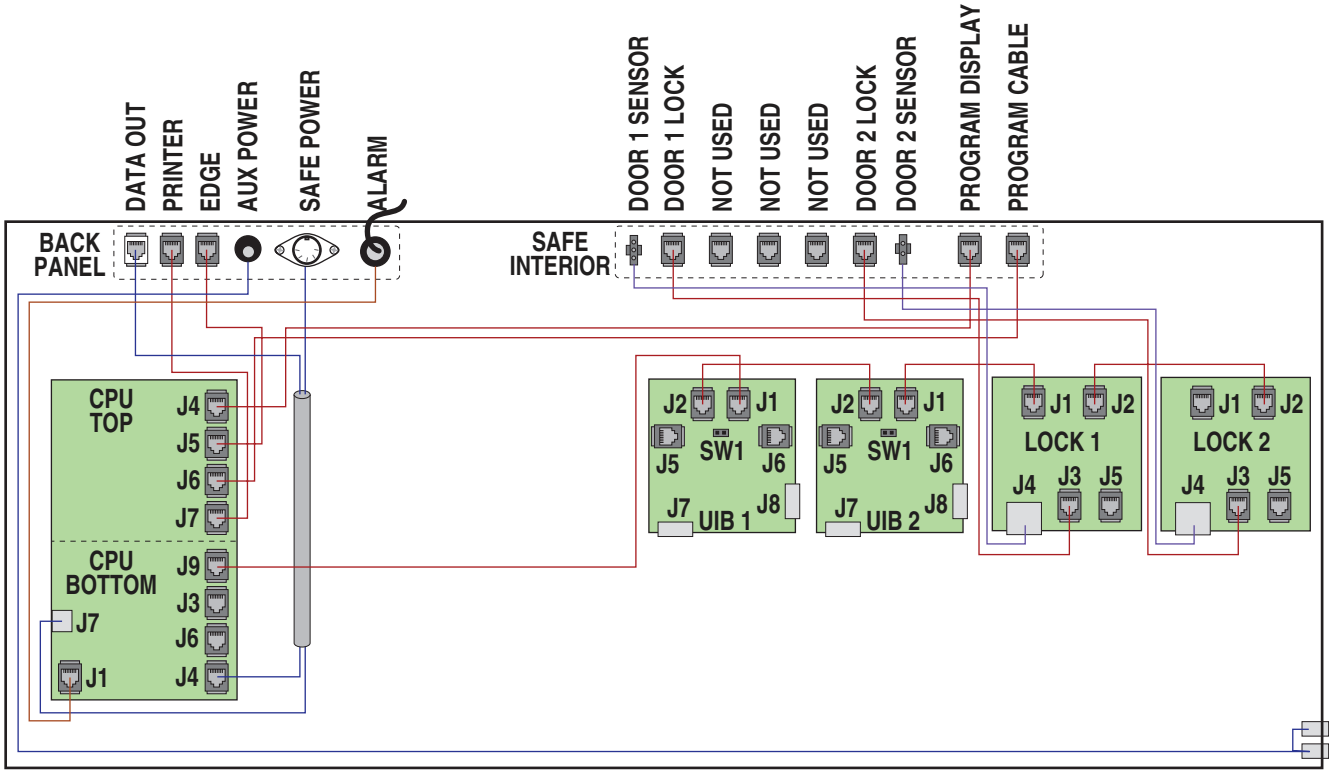
Electronics cans changed so that "C" unit has one "Data Out" port instead of "Data 1" and "Data 2" ports. "R" units also changed so that they now have a "Data In" port, a "Data Out" port, and a "Data End" port. A data bus termination plug is to be inserted in the Data End port on the last "R" unit (V1R, V2R or EPR) on the data bus. NKL also began terminating the internal data bus on all "C" and "R" units at the same time, at SP2008032034.

19 ELECTRICAL SYSTEM

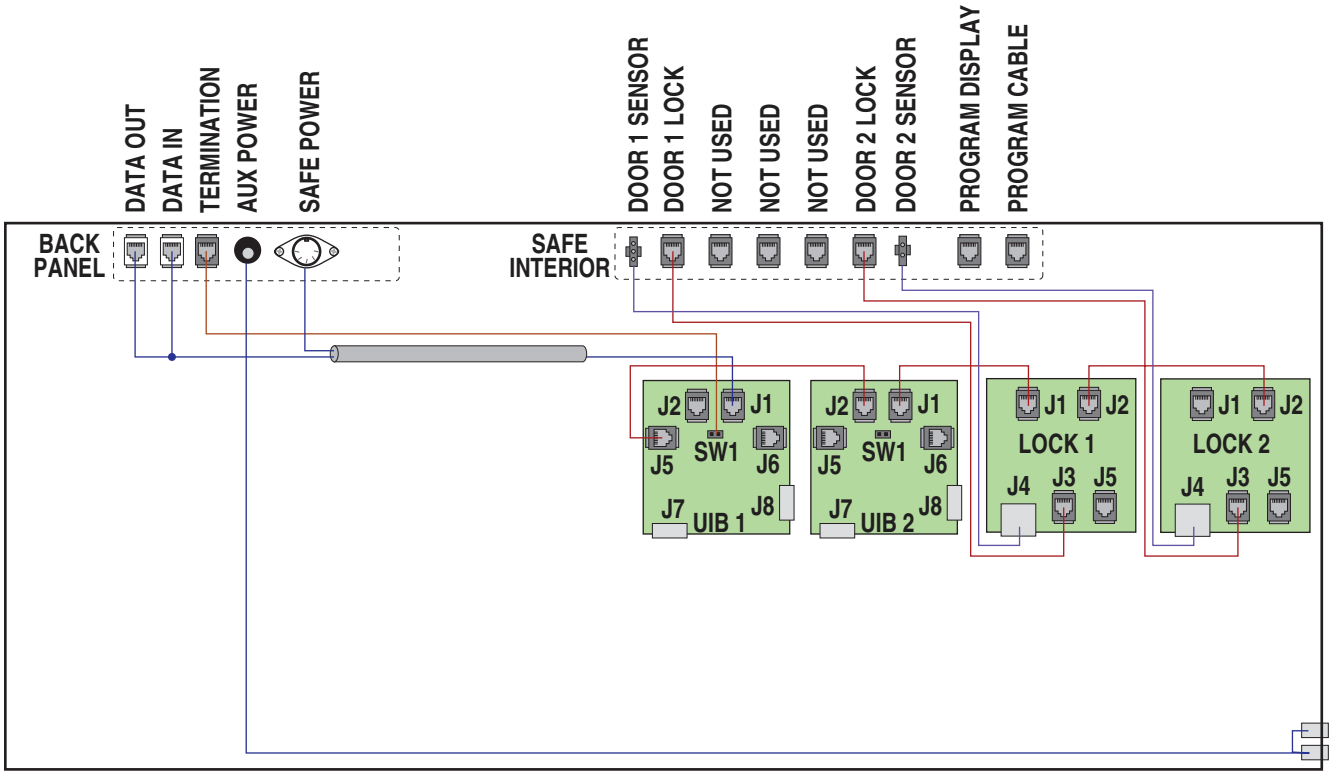


Item	Part	Description
A		Refer to applicable Can section
B	15000373	12 V_{DC} Aux Power Supply Transformer - JCM or CashCode Validators
B	15000206	24 V_{AC} Aux Power Supply Transformer - Mars Validators
C	15000346	External Power Supply Transformer
D	15057203	Validator Power & Data Harness - Mars*
D	15009112	Validator Power & Data Harness - CashCode*
D	15057214	Validator Power & Data Harness - JCM*
E		Refer to applicable validator parts section*
F	15052503	Lower Door Harness
G	800730	ACO Keyswitch
H	15054013	Lower Door Sensor
I	15017000	Lower Door Lock
J	15052508	Upper Door Harness (2-Door safes only)
K	15011000	Upper Door Lock (2-Door safes only)
L	15054013	Upper Door Sensor (2-Door safes only)
		**V1 has one of this part; V2 has two of this part.*

20 ELECTRONICS CANS – BEFORE SP2009XXX
C-UNIT INTERNAL WIRING DIAGRAM



R-UNIT INTERNAL WIRING DIAGRAM



Part	V1C CAN Description
1505AM15	1 Door - Mars
1505AC15	1 Door - CashCode
1505BC15	2 Door - CashCode
1505AJ15	1 Door - JCM
1505BJ15	2 Door - JCM

Part	V1R CAN Description
1505AM13	1 Door - Mars
1505AC13	1 Door - CashCode
1505BC13	2 Door - CashCode
1505AC17	Sidecar - CashCode
1505AJ13	1 Door - JCM
1505BJ13	2 Door - JCM

Part	V2C CAN Description
1505AM16	1 Door - Mars
1505AC16	1 Door - CashCode
1505BC16	2 Door - CashCode
1505AJ16	1 Door - JCM
1505BJ16	2 Door - JCM

Part	V2R CAN Description
1505AM14	1 Door - Mars
1505AC14	1 Door - CashCode
1505BC14	2 Door - CashCode
1505AC18	Sidecar - CashCode
1505AJ14	1 Door - JCM
1505BJ14	2 Door - JCM

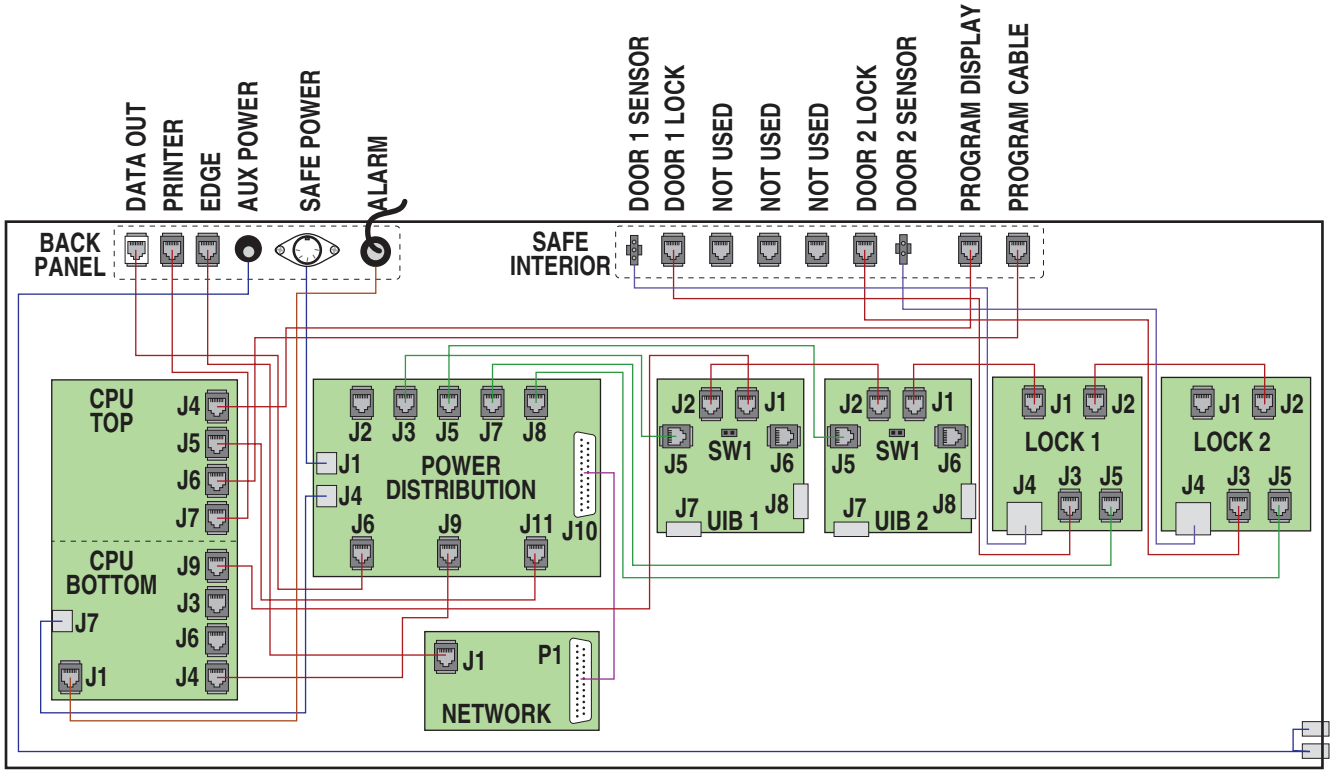
Part	Boards
15058400	CPU Assembly
15057000	UIB* (One if V1, two if V2)
15054000	Lock Board** (One if one door, two if two doors)

Part	Cables***
15052500-C	Main Power/Data Harness
15009110	V1 Aux Power Internal Cable Harness
15009111	V2 Aux Power Internal Cable Harness
15020610	Alarm Cable: CPU BOTTOM J1 / Labeled Bare Wire
15009080	4” RJ/RJ Cable
15009052	6” RJ/RJ Cable
15009081	7” RJ/RJ Cable
15009053	10” RJ/RJ Cable
15009083	10” RJ/RJ Cable, Crossover (Lock Board J3 / Lock Jack)
15009054	16” RJ/RJ Cable
15054021	Lock Sensor Harness (3-wire)
15054023	Lock Sensor Harness (2-wire)

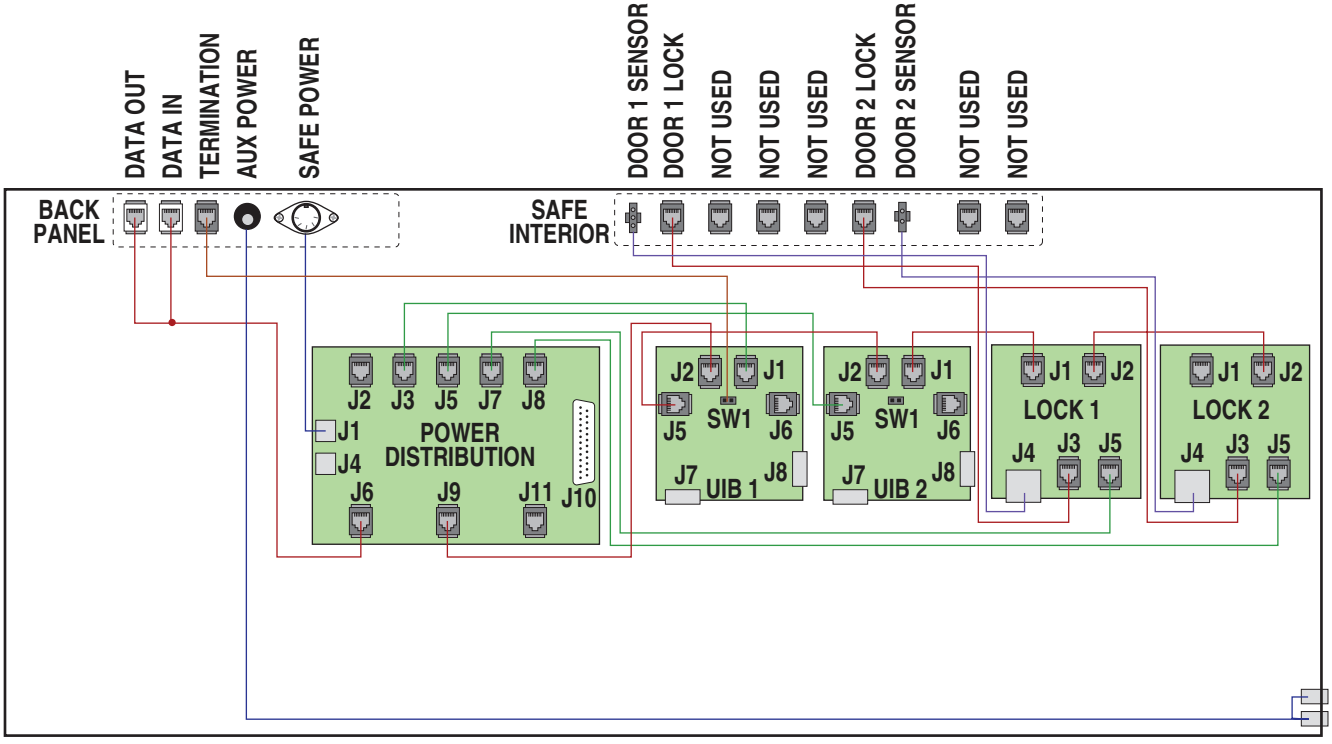
Part	Connectors
15000191S	Shielded RJ45 Right Angle Jack, female/female (DATA IN/OUT jacks)
15000191	Unshielded RJ45 Right Angle Jack, female/female (all other jacks)

**UIB J7 used for Mars or CashCode, J8 used for JCM, J1 and J2 are interchangeable.*
***Lock Board J1 and J2 are interchangeable.*
****Quantities depend on number of validators and doors.*

20 ELECTRONICS CANS – AFTER SP2009XXX
C-UNIT INTERNAL WIRING DIAGRAM



R-UNIT INTERNAL WIRING DIAGRAM



Part	V1C CAN Description
	1 Door - CashCode
	2 Door - CashCode
	1 Door - JCM
	2 Door - JCM

Part	V2C CAN Description
	1 Door - CashCode
	2 Door - CashCode
	1 Door - JCM
	2 Door - JCM

Part	V1R CAN Description
	1 Door - CashCode
	2 Door - CashCode
	Sidecar - CashCode
	1 Door - JCM
	2 Door - JCM

Part	V2R CAN Description
	1 Door - CashCode
	2 Door - CashCode
	Sidecar - CashCode
	1 Door - JCM
	2 Door - JCM

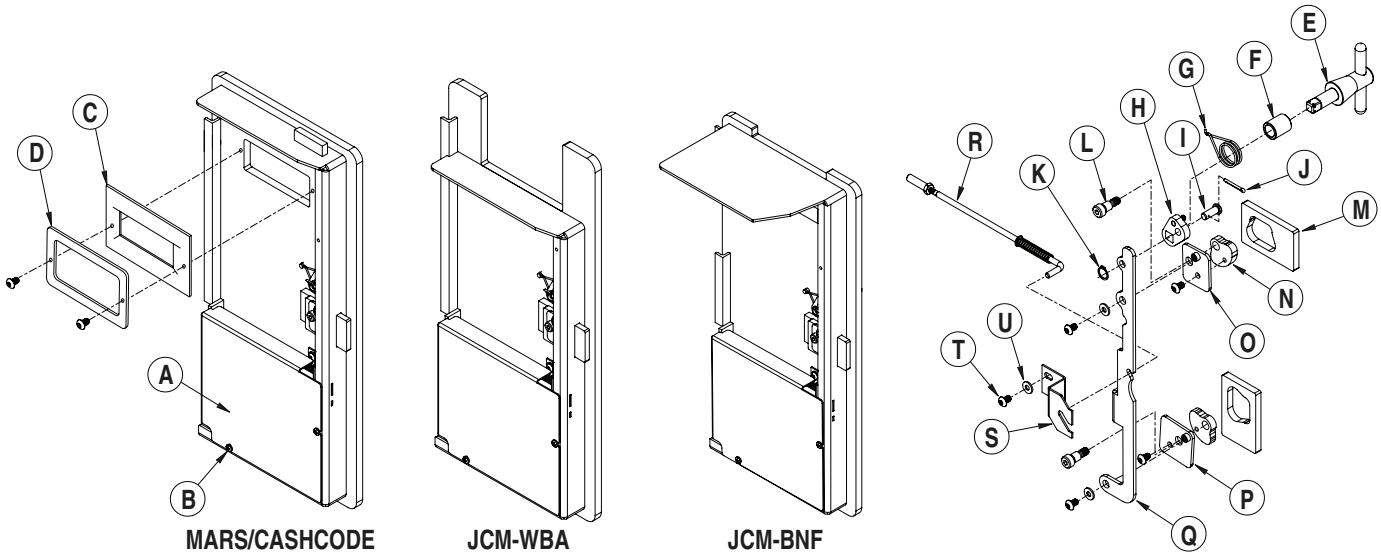
Part	Boards
15058400	CPU Assembly (C-units only)
	Network Interface Board (C-units only)
15058500	Power Distribution Board
15057000	UIB* (One if V1, two if V2)
15054000	Lock Board** (One if one door, two if two doors)

Part	Cables***
15052551	5 Pin Locking DIN / 4 Pin Power Input Harness
15052552	4 Pin / 6 Pin CPU Power Harness
15009110	V1 Aux Power Internal Cable Harness
15009111	V2 Aux Power Internal Cable Harness
15020610	Alarm Cable: CPU BOTTOM J1 / Labeled Bare Wire
15009128-4	4” RJ/RJ Data Cable (blue case)
15009128-6	6” RJ/RJ Data Cable (violet case)
15009128-9	9” RJ/RJ Data Cable (white case)
15009129-6	6” RJ/RJ Power Cable (gray case)
15009129-9	9” RJ/RJ Power Cable (red case)
15009083	10” RJ/RJ Cable, Crossover (Lock Board J3 / Lock Jack, black case)
	DB25 Cable (Power Board J10 / Network Board P1)
15050088	DB25/RJ/Aux Power Harness: Service Use Only (Network Board Programming)
15054021	Lock Sensor Harness (3-wire)
15054023	Lock Sensor Harness (2-wire)

Part	Connectors
15000191S	Shielded RJ45 Right Angle Jack, female/female (DATA IN/OUT jacks)
15000191	Unshield RJ45 Right Angle Jack, female/female (all other jacks)

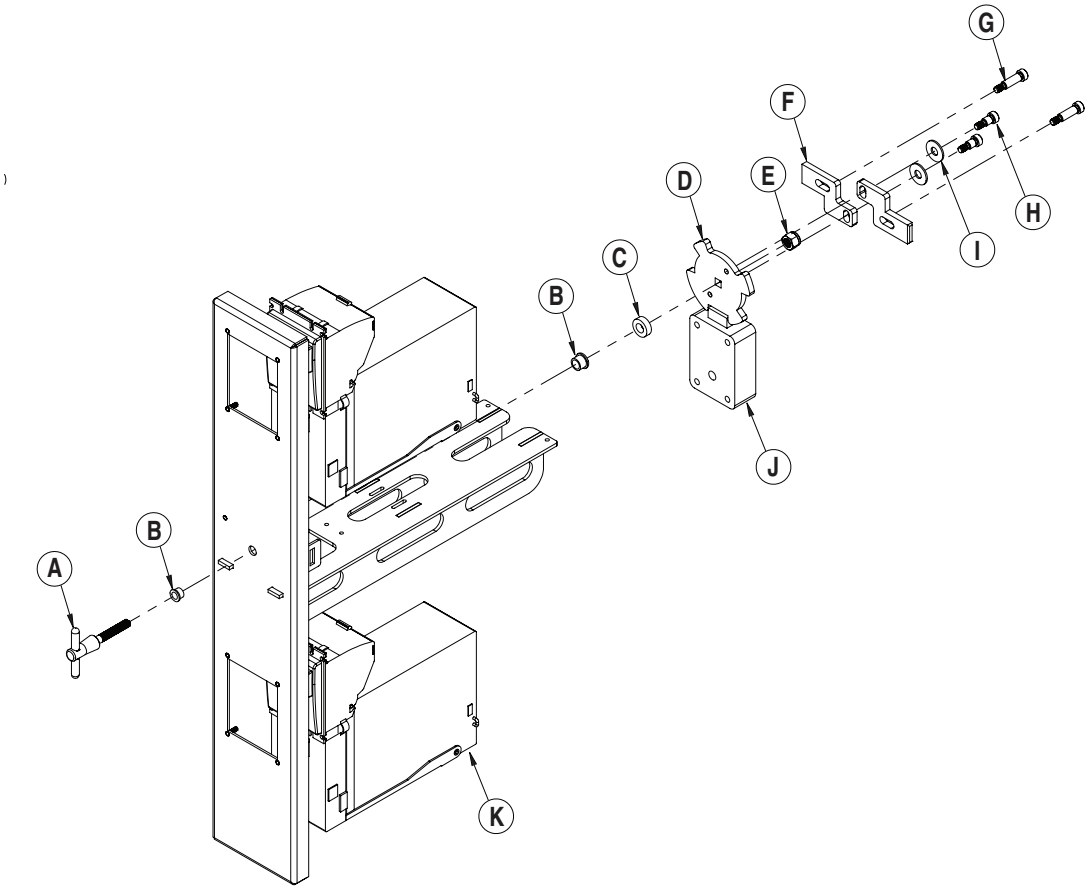
**UIB J7 used for Mars or CashCode, J8 used for JCM, J1 and J2 are interchangeable.*
***Lock Board J1 and J2 are interchangeable.*
****Quantities depend on number of validators and doors.*

21 VALIDATOR COMPARTMENT DOOR HARDWARE



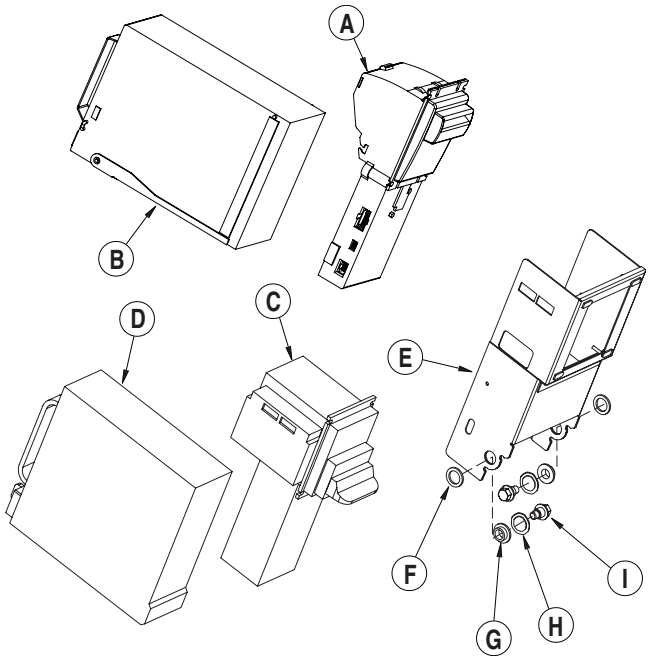
Item	Part	Description
A	800511	V1 Dust Cover
A	800515	V2 Dust Cover
B	G-3235	Screws, Dust Cover (quantity depends on door)
C	800312	Bezel Gasket, Mars
C	800965	Bezel Gasket, CashCode
D	700218	Bezel Gasket Retainer, Mars
D	700510	Bezel Gasket Retainer, CashCode
E	800153	Handle
F	800113	Handle Bushing
G	800218	Handle Spring
H	600029	Handle Actuator
I	HP103	Handle Clevis Pin
J	G-3161	Handle Cotter Pin
K	800152	Handle Retaining Ring
L	800112	Shoulder Bolt (Torque 15-18 ft-lb)
M	700007	Bolt
N	800568	Bolt Actuator
O	600027	Bolt Side Actuator
P	600028	Bolt Reverse Actuator
Q	700983	Bolt Connector Plate, 2-Bolt (JCM-WBA)
Q	700012	Bolt Connector Plate, 3-Bolt (Mars, CashCode, and JCM-BNF)
R	600047	V1 Detent Rod Assembly (rod, spring, adjustment sleeve, nut)
R	600071	V2 Detent Rod Assembly (rod, spring, adjustment sleeve, nut)
	700027	Rod, V1
	700103	Rod, V2
	800186	Spring
	800211	Adjustment Sleeve
	HN700	Adjustment Nut, 8-32
S	700028	Detent Bracket
T	800182	Screw, 10-32 5/16 (Torque 25-30 in-lb)
U	HW102	Washer, Flat #8

22 SIDECAR DOOR HARDWARE



Item	Part	Description
A	3914	Handle
B	801212	Handle Bushing
C	701265	Handle Spacer
D	701264	Bolt Cam
E	HNUT	Locknut
F	701266	Bolt
G	801213	Screw, Shoulder 5/16 x 7/8
H	800112	Screw, Shoulder 5/16 x 3/8
I	G-3120	Washer, Flat
J	15017000	Lock
K		CashCode Validator Assembly (See Section 23)

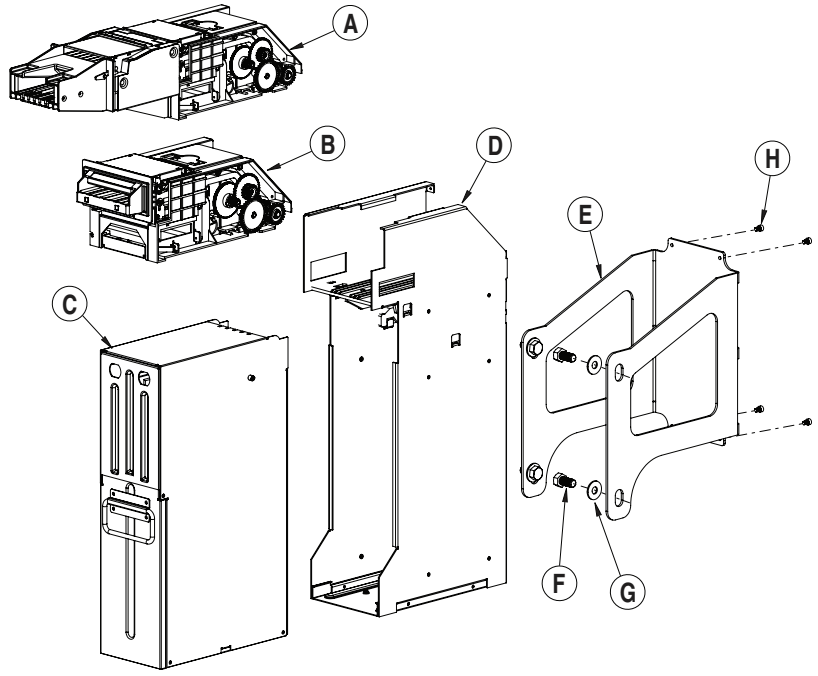
23 MARS / CASHCODE VALIDATOR HARDWARE



Item*	Part	Description
A	15075000	Validator, CashCode USA
A	15075001	Validator, CashCode Canada
B	15075200	Cassette, CashCode 1500 Note
	800805	Hasp lock for CashCode Cassette (optional, not shown)
C	15072400	Validator, Mars 3900
D	15073500	Cassette, Mars 1200 Note NLC, Standard
D	15073200	Cassette, Mars 1200 Note LRC, High Security (optional version)
E	600348	Mounting Bracket, CashCode
E	600015	Mounting Bracket, Mars
F	800146	Washer, Nylon, 11/16 ID (x2)
G	800110	Bushing, Nylon, 1/2 ID (x2)
H	800185	Washer, Wave (x2)
I	800109	Shoulder Bolt (x2)
	06131003	Keps Nut, #10-32, Validator Mounting (x4, Not Shown)

**V1 Models include one of this assembly. V2 Models include two of this assembly.*

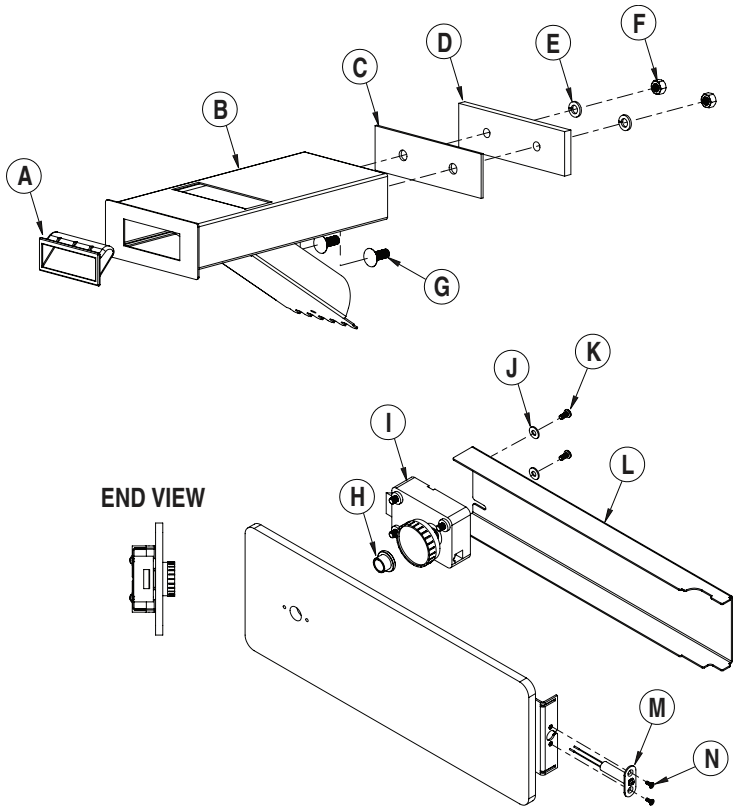
24 JCM BNF / WBA VALIDATOR HARDWARE



Item*	Part	Description
A	15074206	Validator Head, JCM BNF USA (Bulk Note Feed)
A	801041	Validator Head, JCM BNF Canada
	15074207	Bezel, JCM BNF (part of A)
B	15074103	Validator Head, JCM WBA USA (Single Note Feed)
B	15074108	Validator Head, JCM WBA Canada
	801380	Bezel, JCM WBA (part of B)
C	15074202	Cassette, JCM 2000 Note
C	15074100	Cassette, JCM 1000 Note (not shown)
	15073201	Cam Lock (part of C)
D	15074205	Mounting Frame, 2000 Note
D	15074209	Mounting Frame, 1000 Note
E	201273	Mounting Bracket, 2000 Note
F	620-1049	Shoulder Bolt (x4), 3/8-16 x 3/4 (Bracket/Chassis)
G	G-3120	Washer, Flat (x2)
H	800128	Screw, Hex SHCS M4-0.7x6 (x4, Frame/Bracket)

**V1 Models include one of this assembly. V2 Models include two of this assembly.*

25 MANUAL DROP COMPARTMENT HARDWARE



Item	Part	Manual Drop Drawer Parts Description*
A	800551	Plastic Pull Handle, Snap Fit
B	600624	Drawer
C	700851	Drawer Stop
D	700317	Drawer Stop Backer
E	6201050	Washer
F	HN201	Capture Nut
G	HB201	Carriage Bolt
	600626	Complete Assembly (Items A-G)

Item	Part	Manual Drop Door Parts Description**
H	800598	Bushing
I	15011000	Lock
J	HW103	Washer, Flat #10
K	G-3235	Screw, 6-32 3/8
L	700587	V1 Upper Door Cover
L	700602	V2 Upper Door Cover
M	15054013	Sensor
N	800231	Screw, 6-32 5/16

**Manual drop drawer is standard on JSD chassis safes (JCM WBA validator models) only.*
***Manual drop compartment is standard on JSD and JBS chassis safes (JCM validator models).*

26 MISCELLANEOUS

Part	Description
701092	Access Panel (WBA models only)
800182	Screw, 10-32 5/16 (four per Access Panel)
800977	Medeco Cam Lock (WBA models only)
800372	Anchor Kit
801082	APC Uninterruptible Power Supply
800663	OneAC PC180A Power Conditioner
15009077	Printer Cable
15000325	Printer Adapter, RJ45/DB25
800688	Thermal Printer
801383	Cleaning Card
15009076	25’ Cat-5 Data Cable
15009075	50’ Cat-5 Data Cable
15009074	75’ Cat-5 Data Cable
15009073	100’ Cat-5 Data Cable
600133	Dallas Key, XLV
15059020	Display Module
15052520	EPR Power Supply (Non-Biometric)
801692	EPR Biometric Fingerprint Reader
15059635	Cable, EPR Biometric Reader / Display Module

NOTES

NKL TECHNICAL SERVICE
PHONE 800-452-4655
WWW.FIREKING.COM